

Quantifying the Leakage of Quantum Protocols for Classical Two-Party Cryptography^{*}

Louis Salvail¹, Christian Schaffner^{2,3}, and Miroslava Sotáková⁴

¹ Université de Montréal (DIRO), QC, Canada
salvail@iro.umontreal.ca

² Institute for Logic, Language and Computation (ILLC)
University of Amsterdam, The Netherlands
c.schaffner@uva.nl

³ Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands

⁴ Knewton, Inc, NY, USA
gwhitehawk@gmail.com

Abstract. We study quantum protocols among two distrustful parties. By adopting a rather strict definition of correctness—guaranteeing that honest players obtain their correct outcomes only—we can show that every strictly correct quantum protocol implementing a non-trivial *classical* primitive necessarily leaks information to a dishonest player. This extends known impossibility results to all non-trivial primitives. We provide a framework for *quantifying* this leakage and argue that leakage is a good measure for the privacy provided to the players by a given protocol. Our framework also covers the case where the two players are helped by a trusted third party. We show that despite the help of a trusted third party, the players cannot amplify the cryptographic power of any primitive. All our results hold even against quantum honest-but-curious adversaries who honestly follow the protocol but purify their actions and apply a different measurement at the end of the protocol. As concrete examples, we establish lower bounds on the leakage of standard universal two-party primitives such as oblivious transfer.

Keywords: two-party cryptography, quantum protocols, quantum information theory, information leakage.

1 Introduction

Quantum communication allows to implement tasks which are classically impossible. The most prominent example is quantum key distribution [BB84] where two honest players establish a secure key against an eavesdropper. In the two-party setting however, quantum and classical cryptography often show similar limits. Oblivious transfer [Lo97], bit commitment [May97, LC97], and even fair coin tossing [Kit03] are impossible to realize securely both classically and quantumly. On the other hand, quantum cryptography allows for some weaker primitives impossible in the classical world. For example, quantum coin-flipping protocols with maximum bias of $\frac{1}{\sqrt{2}} - \frac{1}{2}$ exist⁵ against any adversary [CK09] while remaining impossible based solely on classical communication. A few other weak primitives are known to be possible with quantum communication. For example, the generation of an additive

^{*} A previous version of this article as appeared at ASIACRYPT 2009 [SSS09].

⁵ In fact, protocols with better bias are known for weak quantum coin flipping [Moc04, Moc05, Moc07].

secret-sharing for the product xy of two bits, where Alice holds bit x and Bob bit y , has been introduced by Popescu and Rohrlich as machines modeling non-signaling non-locality (also called NL-boxes) [PR94]. If Alice and Bob share an EPR pair, they can simulate an NL-box with symmetric error probability $\sin^2 \frac{\pi}{8}$ [PR94, BLM⁺05]. Equivalently, Alice and Bob can implement *1-out-of-2 oblivious transfer* (1-2-OT) privately provided the receiver Bob gets the bit of his choice only with probability of error $\sin^2 \frac{\pi}{8}$ [Amb05]. It is easy to verify that even with such imperfection these two primitives are impossible to realize in the classical world. This discussion naturally leads to the following question:

- Which two-party cryptographic primitives are possible to achieve using quantum communication?

Most standard classical two-party primitives have been shown impossible to implement securely against weak quantum adversaries reminiscent to the classical honest-but-curious (HBC) behavior [Lo97]. The idea behind these impossibility proofs is to consider parties that *purify* their actions throughout the protocol execution. This behavior is indistinguishable from the one specified by the protocol but guarantees that the joint quantum state held by Alice and Bob at any point during the protocol remains pure. The possibility for players to behave that way in any two-party protocol has important consequences. For instance, the impossibility of quantum bit commitment follows from this fact [May97, LC97]: After the commit phase, Alice and Bob share the pure state $|\psi^x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ corresponding to the commitment of bit x . Since a proper commitment scheme provides no information about x to the receiver Bob, it follows that $\text{tr}_A |\psi^0\rangle\langle\psi^0| = \text{tr}_A |\psi^1\rangle\langle\psi^1|$. In this case, the Schmidt decomposition guarantees that there exists a unitary $U_{0,1}$ acting only on Alice's side such that $|\psi^1\rangle = (U_{0,1} \otimes \mathbb{I}_B)|\psi^0\rangle$. In other words, if the commitment is concealing then Alice can open the bit of her choice by applying a suitable unitary transform only to her part. A similar argument allows to conclude that 1-2-OT is impossible [Lo97]: Suppose Alice is sending the pair of bits (b_0, b_1) to Bob through 1-2-OT. Since Alice does not learn Bob's selection bit, it follows that Bob can get bit b_0 before undoing the reception of b_0 and transforming it into the reception of b_1 using a local unitary transform similar to $U_{0,1}$ for bit commitment. For both these primitives, privacy for one player implies that local actions by the other player can transform the honest execution with one input into the honest execution with another input.

In this paper, we investigate the cryptographic power of two-party quantum protocols against players that purify their actions while trying to implement a classical primitive. This *quantum honest-but-curious (QHBC)* behavior is the natural quantum version of classical HBC behavior. This class of adversaries was recently called (*perfectly*) *specious* in [DNS10]. It contains all adversaries that could *prove* to a judge, at any step during a protocol execution, that the joint state (up to an adversary's local computation) is the honest one. We consider classical primitives providing Alice and Bob with random variable X and Y respectively according distribution $P_{X,Y}$. Any such $P_{X,Y}$ models a two-party cryptographic primitive where neither Alice nor Bob provide input. For the purpose of this paper, this model is general enough since any two-party primitive with inputs can be randomized (Alice and Bob pick their input at random) so that its behavior can be described by a suitable joint probability distribution $P_{X,Y}$. If the classical primitive with inputs $f : A \times B \rightarrow W \times Z$ is implemented securely by some protocol π_f then it must also remain secure when Alice's and Bob's private input $(a, b) \in_R A \times B$ is picked uniformly at random. In this case, the

joint probability distribution $P_{X,Y}$ implemented by π_f is simply:

$$P_{X,Y}((a,w),(b,z)) = \frac{\Pr(f(a,b) = (w,z))}{|A| \cdot |B|}.$$

If the randomized version $P_{X,Y}$ is shown to be impossible to implement securely by any quantum protocol then the original primitive with inputs must also be impossible.

Any quantum protocol implementing $P_{X,Y}$ must produce, when both parties purify their actions, a joint pure state $|\psi\rangle \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ that, when subsystems of A and B are measured in the computational basis, leads to outcomes X and Y according the distribution $P_{X,Y}$. Notice that the registers A' and B' only provide the players with extra working space and, as such, do not contribute to the output of the functionality (so parties are free to measure them the way they want). In this paper, we adopt a somewhat strict point of view and define a quantum protocol π for $P_{X,Y}$ to be *strictly correct* if and only if the correct outcomes X, Y are obtained *and* the registers A' and B' do not provide any additional information about Y and X respectively since otherwise π would be implementing a different primitive $P_{XX',YY'}$ rather than $P_{X,Y}$. The state $|\psi\rangle$ produced by any strictly correct protocol for $P_{X,Y}$ is what we call a *quantum embedding* of $P_{X,Y}$. An embedding is called *regular* if registers A' and B' are empty. Any embedding $|\psi\rangle \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ can be produced in the QHBC model by the trivial protocol asking Alice to generate $|\psi\rangle$ before sending the quantum state in $\mathcal{H}_{BB'}$ to Bob. It follows that in the QHBC model, any embedding of $P_{X,Y}$ corresponds to a strictly correct protocol and, since any protocol implementing $P_{X,Y}$ can be purified in the bare model, any strictly correct protocol generates some embedding of $P_{X,Y}$ in the QHBC model.

Notice that if X and Y were provided privately to Alice and Bob—through a trusted third party for instance—then the expected amount of information one party gets about the other party's output is minimal and can be quantified by the Shannon mutual information $I(X;Y)$ between X and Y . Assume that $|\psi\rangle \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ is an embedding of $P_{X,Y}$ produced by a strictly correct quantum protocol. We define the leakage of $|\psi\rangle$ as

$$\Delta_\psi := \max \{ S(X; BB') - I(X; Y), S(Y; AA') - I(Y; X) \}, \quad (1)$$

where $S(X; BB')$ (resp. $S(Y; AA')$) is the information the quantum registers BB' (resp. AA') provide about the output X (resp. Y). That is, the leakage is the maximum amount of extra information about the other party's output given the quantum state held by one party. It turns out that $S(X; BB') = S(Y; AA')$ holds for all embeddings, exhibiting a symmetry similar to its classical counterpart $I(X;Y) = I(Y;X)$ and therefore, the two quantities we are taking the maximum of in (1) coincide.

1.1 Contributions

Our first contribution establishes that the notion of leakage is well behaved. We show that the leakage of any embedding for $P_{X,Y}$ is lower bounded by the leakage of some regular embedding of the same primitive. Thus, in order to lower bound the leakage of any strictly correct implementation of a given primitive, it suffices to minimize the leakage over all its regular embeddings. We also show that the only non-leaking embeddings are the ones for trivial primitives, where a primitive $P_{X,Y}$ is said to be (*cryptographically*) *trivial* if it can be generated by a classical protocol against HBC adversaries⁶. It follows that any quantum

⁶ We are aware of the fact that our definition of triviality encompasses cryptographically interesting primitives like coin-tossing and generalizations thereof for which highly non-trivial protocols

protocol implementing a non-trivial primitive $P_{X,Y}$ must leak information under the sole assumption that it produces (X,Y) with the right joint distribution. This extends known impossibility results for two-party primitives to all non-trivial primitives.

Embeddings of primitives arise from protocols where Alice and Bob have full control over the environment. Having in mind that any embedding of a non-trivial primitive leaks information, it is natural to investigate what tasks can be implemented without leakage with the help of a trusted third party. The notion of leakage can easily be adapted to this scenario. We show that no cryptographic two-party primitive can be implemented without leakage with just one call to the ideal functionality of a weaker primitive⁷. This new impossibility result does not follow from the ones known since they all assume that the state shared between Alice and Bob is pure.

We then turn our attention to the leakage of strictly correct protocols for a few concrete universal primitives. From the results described above, the leakage of any strictly correct implementation of a primitive can be determined by finding the (regular) embedding that minimizes the leakage. In general, this is not an easy task since it requires to find the eigenvalues of the reduced density matrix $\rho_A = \text{tr}_B |\psi\rangle\langle\psi|$ (or equivalently $\rho_B = \text{tr}_A |\psi\rangle\langle\psi|$). As far as we know, no known results allow us to obtain a non-trivial lower bound on the leakage (which is the difference between the mutual information and accessible information) of non-trivial primitives. One reason being that in our setting we need to lower bound this difference with respect to a measurement in one particular basis. However, when $P_{X,Y}$ is such that the bit-length of either X or Y is short, the leakage can be computed precisely. We show that any strictly correct implementation of 1-2-OT necessarily leaks $\frac{1}{2}$ bit. Since NL-boxes and 1-2-OT are locally equivalent, the same minimal leakage applies to NL-boxes [WW05b]. This is a stronger impossibility result than the one by Lo [Lo97] since he assumes perfect/statistical privacy against one party while our approach only assumes strict correctness (while both approaches apply even against QHBC adversaries). We finally show that for Rabin-OT and 1-2-OT of r -bit strings (i.e. ROT^r and $1\text{-}2\text{-OT}^r$ respectively), the leakage approaches 1 exponentially in r . In other words, strictly correct implementations of these two primitives trivialize as r increases since the sender gets almost all information about Bob's reception of the string (in case of ROT^r) and Bob's choice bit (in case of $1\text{-}2\text{-OT}^r$). These are the first quantitative impossibility results for these primitives and the first time the hardness of implementing different flavors of string OT is shown to increase as the strings to be transmitted get longer.

Finally, we note that our lower bounds on the leakage of the randomized primitives also lower-bound the minimum leakage for the standard versions of these primitives⁸ where the players choose their inputs uniformly at random. While we focus on the typical case where the primitives are run with uniform inputs, the same reasoning can be applied to primitives with arbitrary distributions of inputs.

exist [Moc07,CK09]. However, the important fact (for the purpose of this paper) is that all these primitives can be implemented by *trivial* classical protocols against HBC adversaries.

⁷ The weakness of a primitive will be formally defined in terms of entropic monotones for classical two-party computation introduced by Wolf and Wullschleger [WW04], see Section 4.2.

⁸ The definition of leakage of an embedding can be generalized to protocols with inputs, where it is defined as $\max\{\sup_{V_B} S(X; V_B) - I(X; Y), \sup_{V_A} S(V_A; Y) - I(X; Y)\}$, where X and Y involve both inputs and outputs of Alice and Bob, respectively. The supremum is taken over all possible (quantum) views V_A and V_B of Alice and Bob obtained by their (QHBC-consistent) actions (and containing their inputs).

1.2 Related Work

Our framework allows to quantify the minimum amount of leakage whereas standard impossibility proofs as the ones of [LC97, May97, Lo97, AKSW07, BCS12] do not in general provide such quantification since they usually assume privacy for one player in order to show that the protocol must be totally insecure for the other player⁹. By contrast, we derive lower bounds for the leakage of any strictly correct implementation. At first glance, our approach seems contradictory with standard impossibility proofs since embeddings leak the same amount towards both parties. To resolve this apparent paradox it suffices to observe that in previous approaches only the adversary purified its actions whereas in our case both parties do. If a honest player does not purify his actions then some leakage may be lost by the act of irreversibly and unnecessarily measuring some of his quantum registers.

Our results complement the ones obtained by Colbeck in [Col07] for the setting where Alice and Bob have inputs and obtain identical outcomes (called single-function computations). [Col07] shows that in any strictly correct implementation of primitives of a certain form, an honest-but-curious player can access more information about the other party's input than it is available through the ideal functionality. Unlike [Col07], we deal in our work with the case where Alice and Bob do not have inputs but might receive different outputs according to a joint probability distributions. We show that only trivial distributions can be implemented securely in the QHBC model. Furthermore, we introduce a quantitative measure of protocol-insecurity that lets us answer which embedding allow the least effective cheating.

Another notion of privacy in quantum protocols, generalizing its classical counterpart from [CK91, Kus92], is proposed by Klauck in [Kla04]. Therein, two-party quantum protocols with inputs for computing a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, where \mathcal{X} and \mathcal{Y} denote Alice's and Bob's respective input spaces, and privacy against QHBC adversaries are considered. Privacy of a protocol is measured in terms of *privacy loss*, defined for each round of the protocol and fixed distribution of inputs $P_{X', Y'}$ by $S(B; X|Y) = H(X|Y) - S(X|B, Y)$, where B denotes Bob's private working register, and $X := (X', f(X', Y'))$, $Y := (Y', f(X', Y'))$ represent the complete views of Alice and Bob, respectively. Privacy loss of the entire protocol is then defined as the supremum over all joint input distributions, protocol rounds, and states of working registers. In our framework, privacy loss corresponds to $S(X; YB) - I(X; Y)$ from Alice point's of view and $S(Y; XA) - I(X; Y)$ from Bob's point of view. Privacy loss is therefore very similar to our definition of leakage except that it requires the players to get their respective honest outputs. As a consequence, the protocol implementing $P_{X, Y}$ by asking one party to prepare a regular embedding of $P_{X, Y}$ before sending her register to the other party would have no privacy loss. Moreover, the scenario analyzed in [Kla04] is restricted to primitives which provide the same output $f(X, Y)$ to both players. Another difference is that since privacy loss is computed over all rounds of a protocol, a party is allowed to abort which is not considered QHBC in our setting. In conclusion, the model of [Kla04] is different from ours even though the measures of privacy loss and leakage are similar. [Kla04] provides interesting results concerning trade-offs between privacy loss and communication complexity of quantum protocols, building upon similar results of [CK91, Kus92] in the classical scenario.

⁹ Trade-offs between the security for one and the security for the other player have been considered before, but either the relaxation of security has to be very small [Lo97] or the trade-offs are restricted to particular primitives such as commitments [SR01, BCH⁺08] or oblivious transfer [CKS13].

It would be interesting to know whether a similar operational meaning can also be assigned to the new measure of privacy, introduced in this paper.

A result by Künzler et al. [KMR09] shows that two-party functions that are securely computable against active quantum adversaries form a strict subset of the set of functions which are securely computable in the classical HBC model. This complements our result that the sets of securely computable functions in both HBC and QHBC models are the same.

A recent paper by Fehr, Katz, Song, Zhou and Zikas [FKS⁺13] studies our question with respect to the stricter requirements of universal composability. They give classification results for quantum protocols achieving classical primitives with computational and information-theoretic security. Interestingly, classical and quantum protocols seem to be similarly powerful with respect to computational security whereas in the information-theoretic setting, the two landscapes look different.

1.3 Roadmap

In Section 2, we introduce the cryptographic and information-theoretic notions and concepts used throughout the paper. We define, motivate, and analyze the generality of modeling two-party quantum protocols by embeddings in Section 3 and define triviality of primitives and embeddings. In Section 4, we define the notion of leakage of embeddings, show basic properties and argue that it is a reasonable measure of privacy. In Section 5, we explicitly lower bound the leakage of some universal two-party primitives. Finally, in Section 6 we discuss possible directions for future research and open questions.

2 Preliminaries

2.1 Quantum Information Theory

For $x, y \in \{0, 1\}^n$, $\delta_{x,x} = 1$ and $\delta_{x,y} = 0$ if $x \neq y$. In the following, we denote by $\mathcal{U}(A)$ the set of unitary transforms acting in Hilbert space \mathcal{H}_A . Let $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ be an arbitrary pure state of the joint systems A and B . The states of these subsystems are $\rho_A = \text{tr}_B |\psi\rangle\langle\psi|$ and $\rho_B = \text{tr}_A |\psi\rangle\langle\psi|$, respectively. We denote by $S(A)_\psi := S(\rho_A)$ and $S(B)_\psi := S(\rho_B)$ the von Neumann entropy (defined as the Shannon entropy of the eigenvalues of the density matrix) of subsystem A and B respectively. Whenever the quantum state $|\psi\rangle$ is clear from the context, we omit the subscripts from entropic quantities and simply write $S(A)$ and $S(B)$. Since the joint system is in a pure state, it follows from the Schmidt decomposition that $S(A) = S(B)$ (see e.g. [NC00]). Analogously to their classical counterparts, we can define *quantum conditional entropy* $S(A|B) := S(AB) - S(B)$, and *quantum mutual information* $S(A; B) := S(A) + S(B) - S(AB) = S(A) - S(A|B) = S(B) - S(B|A)$. Note that applying a local unitary transform $U = \mathbb{I}_A \otimes U_B$ to the bipartite state ρ_{AB} does not change the mutual information $S(A; B)_\rho = S(A; B)_{U\rho U^\dagger}$, because the spectra of eigenvalues of ρ_A , ρ_B and ρ_{AB} remain the same. Even though $S(A|B)$ can be negative in general, $S(A|B) \geq 0$ is always true if A is a classical register.

Let $R = \{(P_X(x), \rho_R^x)\}_{x \in \mathcal{X}}$ be an ensemble of states ρ_R^x with prior probability $P_X(x)$. This defines a classical-quantum (cq) state ρ_{XR} where the average quantum state is $\rho_R = \sum_{x \in \mathcal{X}} P_X(x) \rho_R^x$. The following lemma states that applying a separate unitary transform to each ρ_R^x does not change the entropies $S(XR)$ and $H(X)$, but it might change $S(R)$.

Lemma 2.1. *Let $\rho_{XR} = \sum_{x \in \mathcal{X}} P_X(x) \rho_R^x$ be a cq-state and let $U_{XR} = \sum_x |x\rangle\langle x|_X \otimes U_R^x$ be a unitary transform acting only on register R , conditioned on the classical value x in X . Then, $S(XR)_{\rho_{XR}} = S(XR)_{U_{XR}\rho_{XR}U_{XR}^\dagger}$ and $H(X)_{\rho_{XR}} = H(X)_{U_{XR}\rho_{XR}U_{XR}^\dagger}$.*

Proof. The density matrix of the cq-state ρ_{XR} is block-diagonal and applying separate unitary transforms U_R^x in every sub-block does not change the overall spectrum of eigenvalues. Hence, the entropy $S(XR)$ remains the same. The second equality follows from the fact that the unitary U_{XR} only acts on register R . \square

The famous result by Holevo upper-bounds the amount of classical information about X that can be obtained by measuring ρ_R :

Theorem 2.2 (Holevo bound [Hol73,Rus02]). *Let Y be the random variable describing the outcome of some measurement applied to ρ_R for $R = \{P_X(x), \rho_R^x\}_{x \in \mathcal{X}}$. Then, $I(X; Y) \leq S(\rho_R) - \sum_x P_X(x) S(\rho_R^x)$, where equality can be achieved if and only if $\{\rho_R^x\}_{x \in \mathcal{X}}$ are simultaneously diagonalizable.*

Note that if all states in the ensemble are pure and all different then in order to achieve equality in the theorem above, they have to form an orthonormal basis of the space they span. In this case, the variable Y achieving equality is the measurement outcome in this orthonormal basis.

2.2 Markov Chains

We say that three classical random variables X, Y, Z with joint distribution P_{XYZ} form a *Markov chain* $X \leftrightarrow Y \leftrightarrow Z$, if X and Z are independent given Y , i.e., $P_{XZ|Y} = P_{X|Y} \cdot P_{Z|Y}$. Equivalent conditions are $P_{X|YZ} = P_{X|Y}$ or $P_{Z|YX} = P_{Z|Y}$ [CT91]. Markov chains with quantum ends have been defined in [DFSS07] and used in subsequent works such as [FS09]. For a ccq-state $\rho_{XYR} = \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_R^{x,y}$, we say that X, Y, R form a Markov chain $X \leftrightarrow Y \leftrightarrow R$, if $\rho_{XYR} = \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_R^y$, i.e., the quantum register R depends only on the classical variable y but not on x .

Lemma 2.3. *For a ccq-state ρ_{XYR} , the following conditions are equivalent:*

1. $X \leftrightarrow Y \leftrightarrow R$
2. $S(X|YR) = S(X|Y)$
3. $S(R|YX) = S(R|Y)$
4. $S(X; YR) = I(X; Y)$.

Proof. For fixed x, y , we can diagonalize $\rho_R^{x,y} = \sum_k \lambda_k^{x,y} |\varphi_k^{x,y}\rangle\langle \varphi_k^{x,y}|_R$. By redefining the random variable Y to be (YK) with joint distribution $P_{X(YK)}(x, yk) = P_{XY}(x, y) \lambda_k^{x,y}$, we can assume without loss of generality that $\rho_R^{x,y} = |\varphi^{x,y}\rangle\langle \varphi^{x,y}|_R$ is a pure state for every fixed x, y . In that case, it is easy to check that $X \leftrightarrow Y \leftrightarrow R$ implies the other three conditions, because $S(XYR) = S(XY)$ and $S(YR) = S(Y)$.

On the other hand, if $X \leftrightarrow Y \leftrightarrow R$ does not hold, there exist $x \neq x'$ and y such that $\rho_R^{x,y} \neq \rho_R^{x',y}$. Hence, there exists a measurement on registers YR that reveals more information about X than just knowing Y , which implies $S(X|YR) \neq S(X|Y)$. The other implications can be shown similarly. \square

2.3 Dependent Part

The following definition introduces a random variable describing the correlation between two random variables X and Y , obtained by collapsing all values x_1 and x_2 for which Y has the same conditional distribution, to a single value.

Definition 2.4 (Dependent part [WW04]). *For two random variables X, Y , let $f_X(x) := P_{Y|X=x}$. Then the dependent part of X with respect to Y is defined as $X \searrow Y := f_X(X)$.*

The dependent part $X \searrow Y$ is the minimum random variable among the random variables computable from X for which $X \leftrightarrow X \searrow Y \leftrightarrow Y$ forms a Markov chain [WW04]. In other words, for any random variable $K = f(X)$ such that $X \leftrightarrow K \leftrightarrow Y$ is a Markov chain, there exists a function g such that $g(K) = X \searrow Y$. Immediately from the definition we get several other properties of $X \searrow Y$ [WW04]: $H(Y|X \searrow Y) = H(Y|X)$, $I(X; Y) = I(X \searrow Y; Y)$, and $X \searrow Y = X \searrow (Y \searrow X)$. The second and the third formula yield $I(X; Y) = I(X \searrow Y; Y \searrow X)$. For two random variables X and Z , we write $X \equiv Z$ if X and Z have the same distributions (over possibly different alphabets). In particular, we write $X \equiv X \searrow Y$ if the random variable X consists only of the dependent part $X \searrow Y$ with respect to Y .

The notion of dependent part has been further investigated in [FWW04, IMNW04, WW05a]. Wullschleger and Wolf have shown that quantities $H(X \searrow Y|Y)$ and $H(Y \searrow X|X)$ are monotones for two-party computation [WW05a]. That is, none of these values can increase during classical two-party protocols. In particular, if Alice and Bob start a protocol from scratch then classical two-party protocols can only produce (X, Y) such that: $H(X \searrow Y|Y) = H(Y \searrow X|X) = 0$, since $H(X \searrow Y|Y) > 0$ if and only if $H(Y \searrow X|X) > 0$ [WW05a]. Conversely, any primitive satisfying $H(X \searrow Y|Y) = H(Y \searrow X|X) = 0$ can be implemented securely in the honest-but-curious (HBC) model. We call such primitives *trivial*¹⁰.

2.4 Connected Components

Another property of a joint probability distribution P_{XY} which we require is the notion of *connected components*, as in [WW04, Def. 1].

Definition 2.5. *Let X and Y be random variables with (disjoint) ranges \mathcal{X} and \mathcal{Y} , distributed according to P_{XY} . Consider the bipartite graph G with vertex set $\mathcal{X} \cup \mathcal{Y}$ such that two vertices $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are connected by an edge iff $P_{XY}(x, y) > 0$ holds. We call the edge sets $\mathcal{C}_1, \dots, \mathcal{C}_\ell$ of connected components of the graph G the connected components of P_{XY} .*

In this way, the joint distribution P_{XY} can be split into ℓ distributions $\{P_{X_j, Y_j}\}_{j=1}^\ell$. For every j , P_{X_j, Y_j} is a distribution with a single component over alphabet $\mathcal{X}_j \times \mathcal{Y}_j$, where \mathcal{X} is the disjoint union of the \mathcal{X}_j and \mathcal{Y} the disjoint union of the \mathcal{Y}_j . We denote by the random variable C the component of XY , resulting in the joint distribution P_{CXY} . Then, $P_C(j) = \sum_{xy \in \mathcal{C}_j} P_{XY}(x, y) = \sum_{x \in \mathcal{X}_j} P_X(x) = \Pr(X \in \mathcal{X}_j) = \sum_{y \in \mathcal{Y}_j} P_Y(y) = \Pr(Y \in \mathcal{Y}_j)$ is the probability that XY ends up in component \mathcal{C}_j (which is the same as the probability that X ends up in \mathcal{X}_j and that Y ends up in \mathcal{Y}_j). Note that C is a deterministic function of X (and also of Y), hence

$$\begin{aligned} I(X; Y) &= H(Y) - H(Y|X) = H(YC) - H(Y|XC) = H(C) + H(Y|C) - H(Y|XC) \\ &= H(C) + I(X; Y|C) . \end{aligned} \quad (2)$$

¹⁰ See Footnote 6 for a caveat about this terminology.

2.5 Purification

All security questions we ask are with respect to (*quantum*) *honest-but-curious* adversaries. In the classical honest-but-curious adversary model (HBC), the parties follow the instructions of a protocol but store all information available to them. Quantum honest-but-curious adversaries (QHBC), on the other hand, are allowed to behave in an arbitrary way that cannot be distinguished from their honest behavior by the other player.

Almost all impossibility results in quantum cryptography rely upon a quantum honest-but-curious behavior of the adversary. This behavior consists in *purifying* all actions of the honest players. Purifying means that instead of invoking classical randomness from a random tape, for instance, the adversary relies upon quantum registers holding all random bits needed. The operations to be executed from the random outcome are then performed quantumly without fixing the random outcomes. For example, suppose a protocol instructs a party to pick with probability p state $|\phi^0\rangle_C$ and with probability $1 - p$ state $|\phi^1\rangle_C$ before sending it to the other party through the quantum channel C . The purified version of this instruction looks as follows: Prepare a quantum register in state $\sqrt{p}|0\rangle_R + \sqrt{1-p}|1\rangle_R$ holding the random process. Add a new register initially in state $|0\rangle_C$ before applying the unitary transform $U : |r\rangle_R|0\rangle_C \mapsto |r\rangle_R|\phi^r\rangle_C$ for $r \in \{0, 1\}$, send register C through the quantum channel and keep register R .

From the receiver's point of view, the purified behavior is indistinguishable from the one relying upon a classical source of randomness because in both cases, the state of register C is $\rho = p|\phi^0\rangle\langle\phi^0| + (1-p)|\phi^1\rangle\langle\phi^1|$. All operations invoking classical randomness can be purified similarly [LC97, May97, Lo97, Ken04]. The result is that measurements are postponed as much as possible and only extract information required to run the protocol in the sense that only when both players need to know a random outcome, the corresponding quantum register holding the random coin will be measured. If both players purify their actions then the joint state at any point during the execution will remain pure, until the very last step of the protocol when the outcomes are measured.

2.6 Secure Two-Party Computation

In Section 5, we investigate the leakage of several universal cryptographic two-party primitives. By universality we mean that any two-party secure function evaluation can be reduced to them. We investigate the completely randomized versions where players do not have inputs but receive randomized outputs instead. Throughout this paper, the term *primitive* usually refers to the joint probability distribution defining its randomized version. Any protocol implementing the standard version of a primitive (with inputs) can also be used to implement a randomized version of the same primitive, with the “inputs” chosen according to an arbitrary fixed probability distribution.

3 Two-Party Protocols and Their Embeddings

3.1 Strict Correctness

In this work, we consider *cryptographic primitives* providing X to honest player Alice and Y to honest player Bob according to a joint probability distribution $P_{X,Y}$. The goal of this section is to define when a protocol π *correctly implements* the primitive $P_{X,Y}$. The first natural requirement is that once the actions of π are purified by both players, measurements

of registers A and B in the computational basis¹¹ provide joint outcome $(X, Y) = (x, y)$ with probability $P_{X,Y}(x, y)$.

Protocol π can use extra registers A' on Alice's and B' on Bob's side providing them with (quantum) working space. The purification of all actions of π therefore generates a pure state $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$. A second requirement for the correctness of the protocol π is that these extra registers are only used as working space, i.e. the final state $|\psi\rangle_{ABA'B'}$ is such that the content of Alice's working register A' does not give her any further information about Bob's output Y than what she can infer from her honest output X and vice versa for B' . Formally, we require that $S(XA'; Y) = I(X; Y)$ and $S(X; YB') = I(X; Y)$. By Lemma 2.3, the two conditions are equivalent to requiring $A' \leftrightarrow X \leftrightarrow Y \leftrightarrow B'$ to be a Markov chain.

Definition 3.1. A protocol π for $P_{X,Y}$ is strictly correct if measuring registers A and B of its final state in the computational basis yields outcomes X and Y with distribution $P_{X,Y}$ and the final state satisfies $S(X; YB') = S(XA'; Y) = I(X; Y)$ where A' and B' denote the extra working registers of Alice and Bob. The state $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$ is called an embedding of $P_{X,Y}$ if it can be produced by the purification of a strictly correct protocol for $P_{X,Y}$.

We would like to point out that our definition of correctness is stronger than the usual classical notion which only requires the correct distribution for the output of the honest players. For example, the trivial classical protocol for the primitive $P_{X,Y}$ in which Alice samples both player's outputs XY , sends Y to Bob, but keeps a copy of Y for herself, is not *strictly correct* because it implements a fundamentally different primitive, namely $P_{XY,Y}$. Definition 3.1 requires that any protocol for $P_{X,Y}$ leaks no information beyond $I(X; Y)$ to any party having measured its output X or Y .

3.2 Regular Embeddings

We call an embedding $|\psi\rangle_{ABA'B'}$ *regular* if the working registers A', B' are empty. Formally, let $\Theta_{n,m} := \{\theta : \{0, 1\}^n \times \{0, 1\}^m \rightarrow [0 \dots 2\pi]\}$ be the set of functions mapping bit-strings of length $m + n$ to real numbers between 0 and 2π .

Definition 3.2. For a joint probability distribution $P_{X,Y}$ where $X \in \{0, 1\}^n$ and $Y \in \{0, 1\}^m$, we define the set

$$\mathcal{E}(P_{X,Y}) := \left\{ |\psi\rangle \in \mathcal{H}_{AB} : |\psi\rangle = \sum_{x \in \{0,1\}^n, y \in \{0,1\}^m} e^{i\theta(x,y)} \sqrt{P_{X,Y}(x,y)} |x, y\rangle_{AB}, \theta \in \Theta_{n,m} \right\},$$

and call any state $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ a regular embedding of the joint probability distribution $P_{X,Y}$.

Clearly, any $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ produces (X, Y) with distribution $P_{X,Y}$ since the probability that Alice measures x and Bob measures y in the computational basis is $|\langle \psi | x, y \rangle|^2 = P_{X,Y}(x, y)$. In order to specify a particular regular embedding one only needs to give the

¹¹ It is clear that every quantum protocol for which the final measurement (providing (x, y) with distribution $P_{X,Y}$ to the players) is not in the computational basis can be transformed into a protocol of the described form by two additional local unitary transformations.

description of the *phase function* $\theta(x, y)$. We denote by $|\psi_\theta\rangle \in \mathcal{E}(P_{X,Y})$ the quantum embedding of $P_{X,Y}$ with phase function θ . The constant function $\theta(x, y) := 0$ for all $x \in \{0, 1\}^n, y \in \{0, 1\}^m$ corresponds to what we call *canonical embedding* $|\psi_0\rangle := \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x, y\rangle_{AB}$.

In Lemma 4.3 below we show that every primitive $P_{X,Y}$ has a regular embedding which is in some sense the most secure among all embeddings of $P_{X,Y}$.

3.3 Trivial Classical Primitives and Trivial Embeddings

In this section, we define *triviality* of classical primitives and (bipartite) embeddings. We show that for any non-trivial classical primitive, its canonical quantum embedding is also non-trivial. Intuitively, a primitive $P_{X,Y}$ is *trivial* if X and Y can be generated by Alice and Bob from scratch in the classical honest-but-curious (HBC) model¹². Formally, we define triviality via an entropic quantity based on the notion of *dependent part* (see Section 2).

Definition 3.3. A primitive $P_{X,Y}$ is called *trivial* if it satisfies $H(X \searrow Y|Y) = 0$, or equivalently, $H(Y \searrow X|X) = 0$. Otherwise, the primitive is called *non-trivial*.

Definition 3.4. A regular embedding $|\psi\rangle_{AB} \in \mathcal{E}(P_{X,Y})$ is called *trivial* if either $S(X \searrow Y|B) = 0$ or $S(Y \searrow X|A) = 0$. Otherwise, we say that $|\psi\rangle_{AB}$ is *non-trivial*.

Notice that unlike in the classical case, $S(X \searrow Y|B) = 0 \Leftrightarrow S(Y \searrow X|A) = 0$ does not hold in general. As an example, consider a shared quantum state where the computational basis corresponds to the Schmidt basis for only one of its subsystems, say for A . Let $|\psi\rangle = \alpha|0\rangle_A|\xi_0\rangle_B + \beta|1\rangle_A|\xi_1\rangle_B$ be such that both subsystems are two-dimensional, $\{|\xi_0\rangle, |\xi_1\rangle\} \neq \{|0\rangle, |1\rangle\}$, $\langle\xi_0|\xi_1\rangle = 0$, and $|\langle\xi_0|0\rangle| \neq |\langle\xi_1|0\rangle|$. We then have $S(X|B) = 0$ and $S(Y|A) > 0$ while $X \equiv X \searrow Y$ and $Y \equiv Y \searrow X$.

To illustrate this definition of triviality, we argue in the following that if a primitive $P_{X,Y}$ has a trivial regular embedding, there exists a classical protocol which generates X, Y securely in the HBC model. Let $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ be trivial and assume without loss of generality that $S(Y \searrow X|A) = 0$. Intuitively, this means that Alice can learn everything possible about Bob's outcome Y (Y could include some private coin-flips on Bob's side, but that is "filtered out" by the dependent part). More precisely, Alice holding register A can measure her part of the shared state to completely learn a realization of $Y \searrow X$, specifying $P_{X|Y=y}$. She then chooses X according to the distribution $P_{X|Y=y}$. An equivalent way of trivially generating (X, Y) classically is the following classical protocol:

1. Alice samples y' from distribution $P_{Y \searrow X}$ and announces the outcome to Bob.
2. Alice samples x from distribution $P_{X|Y \searrow X=y'}$.
3. Bob samples y from distribution $P_{Y|Y \searrow X=y'}$.

Of course, the same reasoning applies in case $S(X \searrow Y|B) = 0$ with the roles of Alice and Bob reversed.

In fact, the following lemma shows that any non-trivial primitive $P_{X,Y}$ has a non-trivial embedding, i.e. there exists a quantum protocol strict-correctly implementing $P_{X,Y}$ while leaking less information to QHBC adversaries than any classical protocol for $P_{X,Y}$ in the HBC model.

Lemma 3.5. If $P_{X,Y}$ is a non-trivial primitive then the canonical embedding $|\psi_0\rangle \in \mathcal{E}(P_{X,Y})$ is also non-trivial.

¹² See Footnote 6 for a caveat about this terminology.

Proof. A non-trivial embedding of $P_{X,Y}$ can be created from a non-trivial embedding of $P_{X \searrow Y, Y \searrow X}$ by applying local unitary transforms. We therefore assume without loss of generality that $X \equiv X \searrow Y$ and $Y \equiv Y \searrow X$. Let

$$|\psi_0\rangle := \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle$$

be the canonical embedding of $P_{X,Y}$. Since $X \equiv X \searrow Y$ and $Y \equiv Y \searrow X$, it holds for any $x_0 \neq x_1$ that $P_{Y|X=x_0} \neq P_{Y|X=x_1}$. Furthermore, since $P_{X,Y}$ is non-trivial, there exist $x_0 \neq x_1$ and y_0 such that $P_{Y|X=x_0}(y_0) > 0$ and $P_{Y|X=x_1}(y_0) = 0$. The state $|\psi_0\rangle$ can be written in the form:

$$|\psi_0\rangle = \sqrt{P_X(x_0)} |x_0\rangle \sum_y \sqrt{P_{Y|X=x_0}(y)} |y\rangle + \sqrt{P_X(x_1)} |x_1\rangle \sum_y \sqrt{P_{Y|X=x_1}(y)} |y\rangle + |\psi'\rangle ,$$

where $\text{tr}(|x_0\rangle\langle x_0| \text{tr}_B |\psi'\rangle\langle\psi'|) = \text{tr}(|x_1\rangle\langle x_1| \text{tr}_B |\psi'\rangle\langle\psi'|) = 0$. Set $|\varphi^{x_b}\rangle := \sum_y \sqrt{P_{Y|X=x_b}(y)} |y\rangle$ for $b \in \{0,1\}$. Since $P_{Y|X=x_0} \neq P_{Y|X=x_1}$, we get that $|\langle\varphi^{x_0}|\varphi^{x_1}\rangle| < 1$. Because all coefficients at $|y\rangle$ in the normalized vectors $|\varphi^{x_0}\rangle$ and $|\varphi^{x_1}\rangle$ are non-negative, and the coefficients at $|y_0\rangle$ are both positive, $\langle\varphi^{x_0}|\varphi^{x_1}\rangle \neq 0$. Therefore, the non-identical states $|\varphi^{x_0}\rangle$ and $|\varphi^{x_1}\rangle$ cannot be perfectly distinguished, which implies that Bob cannot learn whether $X = x_0$ or $X = x_1$ with probability 1. Therefore, the von Neumann entropy on Bob's side $S(B)$ is such that $S(B) < H(X)$. As shown in [WW05a], $H(X \searrow Y|Y) > 0$ implies $H(Y \searrow X|X) > 0$, and we can argue in the same way as above that $S(A) < H(Y)$ from which follows that $|\psi_0\rangle$ is a non-trivial quantum embedding of $P_{X,Y}$. \square

4 The Leakage of Quantum Embeddings

In this section, we formally define the leakage of embeddings and establish properties of the leakage.

4.1 Definition and Basic Properties of Leakage

A perfect implementation of $P_{X,Y}$ simply provides X to Alice and Y to Bob and does nothing else. The expected amount of information that one random variable gives about the other is $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y;X)$. Intuitively, we define the *leakage of a quantum embedding* $|\psi\rangle_{ABA'B'}$ of $P_{X,Y}$ as the larger of the two following quantities: the extra amount of information Bob's quantum registers BB' provide about X and the extra amount Alice's quantum state in AA' provides about Y respectively in comparison to "the minimum amount" $I(X;Y)$.¹³

Definition 4.1. Let $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ be an embedding of $P_{X,Y}$. We define the leakage $|\psi\rangle$ as

$$\Delta_\psi(P_{X,Y}) := \max \{S(X;BB') - I(X;Y), S(AA';Y) - I(X;Y)\} .$$

Furthermore, we say that $|\psi\rangle$ is δ -leaking if $\Delta_\psi(P_{X,Y}) \geq \delta$.

¹³ There are other natural candidates for the notion of leakage such as the difference in difficulty between guessing Alice's output X by measuring Bob's final quantum state B and based on the output of the ideal functionality Y . While such definitions do make sense, they turn out not to be as easy to work with and it is an open question whether the natural properties described later in this section can be established for these notions of leakage as well.

It is easy to see that the leakage is non-negative since $S(X; BB') \geq S(X; \tilde{B})$ for \tilde{B} the result of a quantum operation applied to BB' . Such an operation could be the trace over the extra working register B' and a measurement in the computational basis of each qubit of the part encoding Y , yielding $S(X; \tilde{B}) = I(X; Y)$.

We want to argue that our notion of leakage is a good measure for the privacy of the player's outputs. In the same spirit, we will argue that the minimum achievable leakage for a primitive is related to the "hardness" of implementing it. We start off by proving several basic properties about leakage.

For a general state in $\mathcal{H}_{ABA'B'}$ the quantities $S(X; BB') - I(X; Y)$ and $S(AA'; Y) - I(X; Y)$ are not necessarily equal. Note though that they coincide for regular embeddings $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ produced by a strictly correct protocol (where the work spaces A' and B' are empty): Notice that $S(X; B) = S(X) + S(B) - S(X, B) = H(X) + S(B) - H(X) = S(B)$ and because $|\psi\rangle$ is pure, $S(A) = S(B)$. Therefore, $S(X; B) = S(A; Y)$ and the two quantities coincide. The following lemma states that this actually happens for *all* embeddings and hence, the definition of leakage is symmetric with respect to both players.

Lemma 4.2 (Symmetry). *Let $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ be an embedding of $P_{X,Y}$. Then,*

$$\Delta_\psi(P_{X,Y}) = S(X; BB') - I(X; Y) = S(AA'; Y) - I(X; Y) .$$

Proof. We have already shown that the statement is true in the case where both A' and B' are trivial. In the case where A' is trivial and B' is not, the Markov chain condition implies that $|\psi\rangle$ is of the form

$$|\psi\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB} |\varphi^y\rangle_{B'} ,$$

hence, Bob can fix y_0 and apply a unitary transform $U_{BB'}$ on his part of the system, such that $U_{BB'} |y, \varphi^y\rangle = |y, \varphi^{y_0}\rangle$, and

$$\mathbb{I}_A \otimes U_{BB'} |\psi\rangle_{ABB'} = |\psi^*\rangle_{AB} \otimes |\varphi^{y_0}\rangle_{B'} ,$$

where $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$. Note that the unitary transform $U_{BB'}$ does not change the entropic quantity $S(X; BB')_{|\psi\rangle} = S(X; BB')_{U_{BB'}|\psi\rangle}$. Hence, in the resulting product state, we have that $S(X; BB') - I(X; Y) = S(X; B) - I(X; Y) = S(A; Y) - I(X; Y)$, due to the fact that $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$. An analogous statement holds in the case where B' is trivial and A' is non-trivial.

We now assume that both A' and B' are non-trivial. An embedding of $P_{X,Y}$ can be written as

$$\begin{aligned} |\psi\rangle &= \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB} |\varphi^{x,y}\rangle_{A'B'} \\ &= \sum_j \sqrt{P_C(j)} \sum_{x \in \mathcal{X}_j, y \in \mathcal{Y}_j} \sqrt{P_{X,Y|C=j}(x,y)} |x,y\rangle_{AB} |\varphi^{x,y}\rangle_{A'B'} \\ &= \sum_j \sqrt{P_C(j)} |\psi_j\rangle_{ABA'B'} , \end{aligned}$$

where C denotes the connected component of X, Y (see Section 2.4) and where for any j , $|\psi_j\rangle$ is an embedding of the single-component primitive P_{X_j, Y_j} .

We want to show that

$$S(X; BB')_\psi - I(X; Y) = S(AA'; Y)_\psi - I(X; Y) . \quad (3)$$

Using the reasoning of Equation (2) for the three terms $S(X; BB')$, $I(X; Y)$, $S(AA'; Y)$, Equation (3) is equivalent to¹⁴

$$S(X; BB'|C)_\psi - I(X; Y|C) = S(AA'; Y|C)_\psi - I(X; Y|C)$$

and hence, it suffices to show symmetry for all single-component primitives P_{X_j, Y_j} and their embeddings $|\psi_j\rangle$. For the rest of the proof, we drop the index j for the ease of notation.

Note that $S(X; BB') = H(X) + S(BB') - S(XBB')$ and $S(AA'; Y) = H(Y) + S(AA') - S(AA'Y)$. As $|\psi\rangle$ is a pure state, we have that $S(AA')_\psi = S(BB')_\psi$, and it suffices to show that

$$H(X) - S(XBB')_\psi = H(Y) - S(AY A')_\psi . \quad (4)$$

For every x and y , we can write the bipartite pure state

$$|\varphi^{x,y}\rangle_{A'B'} = \sum_{k=1}^K \sqrt{\lambda_k^{x,y}} |e_k^{x,y}\rangle_{A'} |f_k^{x,y}\rangle_{B'}$$

in Schmidt form. For the reduced density matrices, we obtain

$$\rho_{A'}^{x,y} = \sum_k \lambda_k^{x,y} |e_k^{x,y}\rangle \langle e_k^{x,y}| .$$

Since any embedding $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ of $P_{X,Y}$ is produced by a strictly correct protocol, it satisfies

$$S(XA'; Y) = S(X; YB') = I(X; Y)$$

which is equivalent by Lemma 2.3 to $A' \leftrightarrow X \leftrightarrow Y$ and $X \leftrightarrow Y \leftrightarrow B'$ being Markov chains. It follows that for every x and $y \neq y'$ in the same connected component of P_{XY} , the reduced density matrices $\rho_{A'}^{x,y} = \rho_{A'}^{x,y'} = \rho_{A'}^x$ coincide and therefore, the eigenvalues $\lambda_k^{x,y}$ cannot depend on y . Because of $X \leftrightarrow Y \leftrightarrow B'$, they can neither depend on x . Hence, $|\varphi^{x,y}\rangle = \sum_k \sqrt{\lambda_k} e^{i\theta'(k,x,y)} |e_k^{x,y}\rangle |f_k^{x,y}\rangle$.¹⁵ The phase factors arise from the fact that from a reduced density matrix the global phases of the Schmidt-basis elements cannot be determined.

Let us fix a set of orthogonal states $\{|k\rangle\}_k$. We define the unitary transformation $U_{ABA'B'}$ to map the orthonormal states $\{|e_k^{x,y}\rangle_{A'}\}_k$ into the orthonormal states $\{|k\rangle_{A'}\}_k$, and $\{|f_k^{x,y}\rangle_{B'}\}_k$ into $\{|k\rangle_{B'}\}_k$. Note that $U_{ABA'B'}$ only acts on registers $A'B'$ conditioned

¹⁴ The only step that needs some extra thought is the following: $S(X|BB') = S(X|BB'C)$ holds, because the component C can be determined with certainty by measuring register B with projectors $\{\sum_{y \in \mathcal{Y}_j} |y\rangle \langle y|_B\}_j$.

¹⁵ We note that it is only possible to draw this conclusion within the same connected component. The eigenvalues $\lambda_k^{x,y}$ and $\lambda_k^{x',y'}$ for x, y and x', y' not in the same connected component of P_{XY} cannot be related to each other.

on the x -value in A and the y -value in B . Applying $U_{ABA'B'}$ to $|\psi\rangle$ results into state

$$\begin{aligned} |\chi\rangle &= \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB} \sum_k \sqrt{\lambda_k} e^{i\theta'(k,x,y)} |k,k\rangle_{A'B'} \\ &= \sum_k \sqrt{\lambda_k} \left(\sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta'(k,x,y)} |x,y\rangle \right) |k,k\rangle \\ &= \sum_k \sqrt{\lambda_k} |\chi_k\rangle_{AB} \otimes |k,k\rangle_{A'B'} , \end{aligned}$$

where each $|\chi_k\rangle_{AB} \in \mathcal{E}(P_{X,Y})$. The cq-q-state $\sigma_{XBB'}$ can now be written in the form:

$$\sigma_{XBB'} = \sum_x P_X(x) |x\rangle\langle x| \otimes \sum_k \lambda_k |\gamma_k^x, k\rangle\langle \gamma_k^x, k| ,$$

where $|\gamma_k^x\rangle = \sum_y \sqrt{P_{Y|X=x}} e^{i\theta'(k,x,y)} |y\rangle$. Due to the second register, the states $|\gamma_k^x, k\rangle$ are mutually orthogonal for each x . Therefore, for each x ,

$$S\left(\sum_k \lambda_k |\gamma_k^x, k\rangle\langle \gamma_k^x, k|\right) = H(\lambda_1, \dots, \lambda_K) .$$

As a result we get that

$$S(XBB')_\chi = H(X) + \sum_x P_X(x) H(\lambda_1, \dots, \lambda_K) = H(X) + H(\lambda_1, \dots, \lambda_K)$$

and analogously,

$$S(AA'Y)_\chi = H(Y) + H(\lambda_1, \dots, \lambda_K) .$$

Equation (4) now follows by applying Lemma 2.1 in the first and last step of the following equations.

$$\begin{aligned} H(X) - S(XBB')_\psi &= H(X) - S(XBB')_\chi \\ &= -H(\lambda_1, \dots, \lambda_K) \\ &= H(Y) - S(AY A')_\chi \\ &= H(Y) - S(AY A')_\psi . \end{aligned}$$

□

If a primitive $P_{X,Y}$ has multiple connected components and $|\psi_j\rangle$ are (not necessarily regular) embeddings of P_{X_j,Y_j} , then the state $|\psi\rangle := \sum_j \sqrt{P_C(j)} |\psi_j\rangle$ is an embedding of $P_{X,Y}$ with leakage

$$\begin{aligned} \Delta_\psi(P_{X,Y}) &= S(X; BB')_\psi - I(X; Y) = S(X; BB'|C)_\psi - I(X; Y|C) \\ &= \sum_j P_C(j) \Delta_{\psi_j}(P_{X_j,Y_j}) , \end{aligned} \tag{5}$$

by the same reasoning as in the previous proof (along the lines of Equation (2)). Any party can determine the active component without disturbing the state once the other party

got his/her output (see Footnote 14). Therefore, measuring the component C can be done without changing the amount of information the state contains about the other party's output. Hence, we can always assume that the parties know the current component in use.

The next lemma shows that the leakage of an embedding for a given primitive is always lower-bounded by the leakage of some regular embedding of the same primitive, which simplifies the calculation of lower bounds for the leakage of embeddings.

Lemma 4.3. *For every embedding $|\psi\rangle$ of a primitive $P_{X,Y}$, there exists $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$ such that $\Delta_\psi(P_{X,Y}) \geq \Delta_{\psi^*}(P_{X,Y})$.*

Proof. In the case where A' and B' are both trivial, then $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ is a regular embedding and the statement holds trivially. In the case where A' is trivial and B' is not, we have shown at the beginning of the proof of Lemma 4.2 that an embedding $|\psi\rangle$ of $P_{X,Y}$ is locally equivalent to a state $|\psi'\rangle_{AB} \otimes |\sigma\rangle_{B'}$ for $|\psi'\rangle \in \mathcal{E}(P_{X,Y})$ and a pure state $|\sigma\rangle_{B'}$. An analogous statement holds if B' is trivial and A' is not. Therefore, in these two cases we get for some $|\psi'\rangle \in \mathcal{E}(P_{X,Y})$ that $\Delta_\psi(P_{X,Y}) = \Delta_{\psi'}(P_{X,Y})$.

Now assume that both A' and B' are non-trivial and that $P_{X,Y}$ has multiple connected components. As in the proof of Lemma 4.2, the state $|\psi\rangle_{ABA'B'}$ can be written as

$$|\psi\rangle_{ABA'B'} = \sum_j \sqrt{P_C(j)} |\psi_j\rangle_{ABA'B'} ,$$

where $|\psi_j\rangle$ is an embedding of P_{X_j,Y_j} , the primitive corresponding to the j th connected component of $P_{X,Y}$. Let us assume for now that the lemma holds for single-component primitives. In that case, we get for every j and embedding $|\psi_j\rangle$ a regular embedding $|\psi_j^*\rangle \in \mathcal{E}(P_{X_j,Y_j})$ such that $\Delta_{\psi_j}(P_{X_j,Y_j}) \geq \Delta_{\psi_j^*}(P_{X_j,Y_j})$. We define $|\psi^*\rangle = \sum_j \sqrt{P_C(j)} |\psi_j^*\rangle$ and conclude that

$$\Delta_\psi(P_{X,Y}) = \sum_j P_C(j) \Delta_{\psi_j}(P_{X,Y}) \geq \sum_j P_C(j) \Delta_{\psi_j^*}(P_{X,Y}) = \Delta_{\psi^*}(P_{X,Y}) ,$$

where the equalities are due to Equation (5).

It remains to show the lemma for single-component primitives $P_{X,Y}$. The state $|\psi\rangle_{ABA'B'}$ is of the form established in the proof of Lemma 4.2:

$$|\psi\rangle_{ABA'B'} = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB} \otimes \sum_k \sqrt{\lambda_k} e^{i\theta(k,x,y)} |e_k^{x,y}\rangle_{A'} |f_k^{x,y}\rangle_{B'} . \quad (6)$$

Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_t)$ be an ordering of all eigenvalues $\{\lambda_k\}_k$ each repeated as many times as their multiplicity. Let $F_{x,y} = \{f_k^{x,y}\}_k$ be the set of eigenvectors in B' for each pair (x,y) . Since $X \leftrightarrow Y \leftrightarrow B'$ is a Markov chain, the eigenvectors $f_k^{x,y}$ can be chosen such that $F_{x,y} = F_{x',y} =: F_y$ for any x, x', y in the same connected component. Let us fix an ordering of the elements of F_y , $\langle F_y \rangle = \langle f_1^y, f_2^y, \dots, f_t^y \rangle$, such that eigenvector f_h^y has eigenvalue λ_h whenever $y \in \mathcal{Y}$.¹⁶

¹⁶ The Markov chain condition guarantees that a single ordering $\langle F_y \rangle$ suffices in the following sense: two eigenvectors $f_k^{x,y} \in F_{x,y}$ and $f_{k'}^{x',y} \in F_{x',y}$ such that $f_k^{x,y} = f_{k'}^{x',y} = f_h^y$ for some $f_h^y \in F_y$ necessarily have the same eigenvalue λ_h .

Consider the (incomplete) projective measurement $\mathcal{M} = \{\mathbb{Q}_h\}_h$ with measurement operators

$$\mathbb{Q}_h = \sum_{y \in \mathcal{Y}} |y\rangle\langle y|_B \otimes |f_h^y\rangle\langle f_h^y|_{B'} .$$

Now, suppose that \mathcal{M} is applied to registers BB' of $|\psi\rangle_{ABA'B'}$. It is easy to verify that with probability λ_h , outcome h will be obtained and the state will collapse to:

$$|\psi_h\rangle_{ABA'B'} = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB} \otimes e^{i\theta(k(h,x,y),x,y)} |e_{k(h,x,y)}^{x,y}\rangle_{A'} \otimes |f_h^y\rangle_{B'} ,$$

where $k(h,x,y)$ is the index such that $|e_{k(h,x,y)}^{x,y}\rangle$ is associated with $|f_h^y\rangle$ in the Schmidt decomposition (6) when $X = x$ and $Y = y$. Notice that $|\psi_h\rangle$ is an embedding of $P_{X,Y}$. Let $U_h \in \mathcal{U}(BB')$ be the local unitary transform on BB' defined as:

$$U_h |y\rangle_B |f_h^y\rangle_{B'} = |y\rangle_B |\mathbf{0}\rangle_{B'} ,$$

and let $|\hat{\psi}_h\rangle = (\mathbb{I}_{AA'} \otimes U_h) |\psi_h\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} |x,y\rangle_{AB} \otimes e^{i\theta(k,x,y)} |e_k^{x,y}\rangle_{A'} |\mathbf{0}\rangle_{B'}$ be an embedding of $P_{X,Y}$ locally equivalent to $|\psi_h\rangle$ but with a trivial register B' .

Let us put things together:

$$S(X; BB')_\psi \geq S(X; BB')_{\sum_h \lambda_h |\psi_h\rangle\langle\psi_h|} \quad (7)$$

$$\begin{aligned} &= \sum_h \lambda_h S(X; BB')_{\psi_h} \\ &\geq \min_h S(X; BB')_{\psi_h} \\ &= S(X; BB')_{\hat{\psi}_{h^*}} , \end{aligned} \quad (8)$$

where (7) follows from the fact that the local measurement \mathcal{M} does not increase mutual information [NC00, Theorem 11.15(3)], and (8) follows since $|\hat{\psi}_h\rangle$ is locally equivalent to $|\psi_h\rangle$ for all h . Since $|\hat{\psi}_{h^*}\rangle$ is an embedding of $P_{X,Y}$ with register B' being trivial, we can use the reasoning from the beginning of the proof that $|\hat{\psi}_{h^*}\rangle$ is locally equivalent to a state $|\psi^*\rangle_{AB} \otimes |\sigma\rangle_{B'}$ with $|\psi^*\rangle \in \mathcal{E}(P_{X,Y})$. By Lemma 4.2, the same proof applies to $S(Y; AA')_\psi$. \square

So far, we have defined the leakage of an embedding of a primitive. We now define the leakage of a primitive the natural way:

Definition 4.4. We define the leakage of a primitive $P_{X,Y}$ as the minimal leakage among all protocols strict-correctly implementing $P_{X,Y}$. Formally,

$$\Delta_{P_{X,Y}} := \min_{|\psi\rangle} \Delta_\psi(P_{X,Y}) ,$$

where the minimization is over all embeddings $|\psi\rangle$ of $P_{X,Y}$.

Notice that the minimum in the previous definition is well-defined, because by Lemma 4.3, it is sufficient to minimize over regular embeddings $|\psi\rangle \in \mathcal{E}(P_{X,Y})$. Furthermore, the function $\Delta_\psi(P_{X,Y})$ is continuous on the compact (i.e. closed and bounded) set $[0, 2\pi]^{|\mathcal{X} \times \mathcal{Y}|}$ of complex phases corresponding to elements $|x,y\rangle_{AB}$ in the formula for $|\psi\rangle_{AB} \in \mathcal{E}(P_{X,Y})$ and therefore it achieves its minimum.

The following theorem shows that the leakage of any embedding of a primitive $P_{X,Y}$ is lower-bounded by the minimal leakage achievable for primitive $P_{X \searrow Y, Y \searrow X}$ (which due to Lemma 4.3 is achieved by a regular embedding).

Theorem 4.5. *For any primitive $P_{X,Y}$, $\Delta_{P_{X,Y}} \geq \Delta_{P_{X \searrow Y, Y \searrow X}}$.*

Proof. In fact, the random variables $X \searrow Y$ and $Y \searrow X$ in the claim can be replaced by any variables X' and Y' with the property that $X \leftrightarrow X' \leftrightarrow Y$ and $X \leftrightarrow Y' \leftrightarrow Y$ are Markov chains, and that $Y' = f_Y(Y)$ and $X' = f_X(X)$ for some deterministic functions f_Y and f_X . For such random variables we then have $I(X'; Y') = I(X; Y)$. Therefore, showing that for $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ with the lowest leakage among all regular embeddings of $P_{X,Y}$ (regularity follows from Lemma 4.3) and for some $|\psi^*\rangle \in \mathcal{E}(P_{X',Y'})$, it holds that

$$S(A)_\psi - I(X; Y) = \Delta_\psi(P_{X,Y}) \geq \Delta_{\psi^*}(P_{X',Y'}) = S(A)_{\psi^*} - I(X'; Y')$$

is equivalent to proving $S(A)_\psi \geq S(A)_{\psi^*}$. First, we show that there exists $|\tilde{\psi}\rangle \in \mathcal{E}(P_{X,Y'})$ such that $S(A)_\psi \geq S(A)_{\tilde{\psi}}$, i.e. $\Delta_\psi(P_{X,Y}) \geq \Delta_{\tilde{\psi}}(P_{X,Y'})$. The existence of $|\psi^*\rangle$ such that $\Delta_{\tilde{\psi}}(P_{X,Y'}) \geq \Delta_{\psi^*}(P_{X',Y'})$ follows from an analogous argument.

State $|\psi\rangle$ can be written in the form:

$$|\psi\rangle = \sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta(x,y)} |x,y\rangle_{AB}.$$

For any realization y' of Y' , let $O_{y'}$ be the set of elements y which are mapped to y' under $f_Y(\cdot)$, i.e. $O_{y'} := \{y : f_Y(y) = y'\}$. Let g denote the bijection mapping tuples $(y', j_y) \in Y' \times O_{y'}$ back to y . There exists an isometry U on Bob's side such that

$$\begin{aligned} (\mathbb{I}_A \otimes U)|\psi\rangle_{AB} &= \sum_{x,y} \sqrt{P_{X,Y}(x,y)} e^{i\theta(x,y)} |x, f_Y(y)j_y\rangle_{A\tilde{B}\tilde{B}^\perp} \\ &= \sum_{x,y'} \sqrt{P_{X,Y'}(x,y')} |x, y'\rangle_{A\tilde{B}} \sum_{j \in O_{y'}} \sqrt{P_{Y|Y'=y'}(g(y', j))} e^{i\theta(x, g(y', j))} |j\rangle_{\tilde{B}^\perp}, \end{aligned} \quad (9)$$

where $\mathcal{H}_{\tilde{B}\tilde{B}^\perp} \cong \mathcal{H}_B$.

Our goal for the rest of the proof is to transform the register containing j into a form where the order of the summations over (x, y') and j in (9) can be reversed to get a state of the form

$$|\varphi\rangle = \frac{1}{\sqrt{t}} \sum_{j=1}^t |\hat{\psi}_j\rangle_{A\tilde{B}} |j\rangle_{B'}, \quad (10)$$

where t is some normalization factor and each $|\hat{\psi}_j\rangle$ is in $\mathcal{E}(P_{X,Y'})$. Due to concavity of the von Neumann entropy, we can then argue that

$$\frac{1}{t} \sum_j S(\text{tr}_{\tilde{B}B'} |\hat{\psi}_j\rangle\langle\hat{\psi}_j|) \leq S\left(\frac{1}{t} \sum_j \text{tr}_{\tilde{B}B'} |\hat{\psi}_j\rangle\langle\hat{\psi}_j|\right) = S(\text{tr}_{\tilde{B}B'} |\varphi\rangle\langle\varphi|) = S(A)_\varphi. \quad (11)$$

Hence, there exists a j such that $|\tilde{\psi}_j\rangle \in \mathcal{E}(P_{X,Y'})$ and $S(A)_{\tilde{\psi}_j} \leq S(A)_\varphi = S(A)_\psi$, proving the claim.

Let us fix $\delta > 0$ and we show the existence of an embedding $|\tilde{\psi}_j\rangle \in \mathcal{E}(P_{X,Y'})$ such that $S(A)_{\tilde{\psi}_j} \leq S(A)_\psi + \delta$. In order to reverse the order of summation in (9), we show the existence of an isometry W on Bob's system such that

$$|\hat{\varphi}\rangle := (\mathbb{I}_A \otimes W)(\mathbb{I}_A \otimes U)|\psi\rangle_{AB} = \frac{1}{\sqrt{t}} \sum_{z=1}^t |\hat{\psi}_z\rangle_{A\tilde{B}} |z\rangle_{B'},$$

where each $|\hat{\psi}_z\rangle$ is a quantum embedding of a primitive $P_{\hat{X},\hat{Y}}$ that is ε -close (in statistical distance) to the primitive $P_{X,Y'}$.

The idea is for a given y' and $j \in O_{y'}$ to “slice up” the term $|j\rangle_{\tilde{B}^\perp}$ with weight $\sqrt{P_{Y|Y'=y'}(g(y',j))}$ into a lot of very small pieces of weight $1/\sqrt{t}$ by letting W map $|j\rangle_{\tilde{B}^\perp}$ into superpositions $\sum_z |z\rangle_{B'}$, where $t \in \mathbb{N}$ is a large natural number to be determined later as a function of δ . More formally, let us fix y' and denote the elements of the set $O_{y'}$ as $\{1, 2, \dots, k\}$. As a shorthand, we use $p_j := P_{Y|Y'=y'}(g(y',j))$ and note that $\sum_{j=1}^k p_j = 1$. We define $n_j := \lceil t \cdot p_j \rceil$ to be the natural number of pieces required to approximate $p_j \approx \frac{n_j}{t}$ for large t . Let $t_0 := 0$ and $t_j := \sum_{i \leq j} n_i$. Then, we define W to map $|j\rangle_{\tilde{B}^\perp}$ to $\frac{1}{\sqrt{n_j}} \sum_{z=t_{j-1}+1}^{t_j} |z\rangle$ and get

$$\begin{aligned} |\hat{\phi}\rangle &= (\mathbb{I}_A \otimes W) \sum_{x,y'} \sqrt{P_{X,Y'}(x,y')} |x,y'\rangle_{A\tilde{B}} \sum_{j \in O_{y'}} \sqrt{p_j} e^{i\theta(x,g(y',j))} |j\rangle_{\tilde{B}^\perp} \\ &= \sum_{x,y'} \sqrt{P_{X,Y'}(x,y')} |x,y'\rangle_{A\tilde{B}} \sum_{j \in O_{y'}} \sqrt{\frac{p_j}{n_j}} e^{i\theta(x,g(y',j))} \sum_{z=t_{j-1}+1}^{t_j} |z\rangle, \end{aligned}$$

It is not hard to verify [Sot08] that $\frac{p_j}{n_j}$ can be written as $\frac{1}{t} + \frac{\varepsilon(y',z)}{t^2}$ where the error $|\varepsilon(y',z)| \leq c$ is upper bounded by a constant c independent of t . Then, we get

$$\begin{aligned} |\hat{\phi}\rangle &= \sum_{x,y'} \sqrt{P_{X,Y'}(x,y')} |x,y'\rangle_{A\tilde{B}} \sum_{z=1}^t \sqrt{\frac{1}{t} + \frac{\varepsilon(y',z)}{t^2}} e^{i\theta'(x,y',z)} |z\rangle_{B'} \\ &= \frac{1}{\sqrt{t}} \sum_{z=1}^t \left(\sum_{x,y'} e^{i\theta'(x,y',z)} \sqrt{1 + \frac{\varepsilon(y',z)}{t}} \sqrt{P_{X,Y'}(x,y')} |x,y'\rangle_{A\tilde{B}} \right) |z\rangle_{B'} \\ &= \frac{1}{\sqrt{t}} \sum_{z=1}^t |\hat{\psi}_z\rangle_{A\tilde{B}} |z\rangle_{B'}, \end{aligned}$$

where $\theta'(x,y',z) = \theta(x,y)$ for y corresponding to (y',z) . Using the reasoning from (11), we derive the existence of a z , such that the state $|\hat{\psi}_z\rangle \in \mathcal{E}(P_{\hat{X},\hat{Y}})$ is a regular embedding of a primitive $P_{\hat{X},\hat{Y}}$ that is $\varepsilon(t)$ -close to $P_{X,Y'}$ and $\varepsilon(t) \rightarrow 0$ when $t \rightarrow \infty$. Furthermore, we have that $S(A)_{\hat{\psi}_z} \leq S(A)_\psi$. As $|\hat{\psi}_z\rangle$ is a regular embedding, we can write $|\hat{\psi}_z\rangle = \sum_{\hat{x},\hat{y}} \sqrt{P_{\hat{X},\hat{Y}}(\hat{x},\hat{y})} e^{i\hat{\theta}(\hat{x},\hat{y})} |\hat{x}\rangle |\hat{y}\rangle$ for some phase function $\hat{\theta}(\hat{x},\hat{y})$. We define the desired state $|\tilde{\psi}\rangle \in \mathcal{E}(P_{X,Y'})$ as $|\tilde{\psi}\rangle := \sum_{x,y} \sqrt{P_{X,Y'}(x,y)} e^{i\hat{\theta}(x,y)} |x\rangle |y\rangle$. We can choose t large enough such that the distance $\| |\hat{\psi}_z\rangle - |\tilde{\psi}\rangle \|$ is arbitrarily small and hence, by the continuity of the von Neumann entropy, also their entropies $S(A)$ differ by at most δ . Hence, $S(A)_{\tilde{\psi}} \leq S(A)_{\hat{\psi}_z} + \delta \leq S(A)_\psi + \delta$, which is what we wanted to show. \square

4.2 Leakage as Measure of Privacy and Hardness of Implementation

The main results of this section are consequences of the Holevo bound (Theorem 2.2).

Theorem 4.6. *If a two-party strictly correct quantum protocol for $P_{X,Y}$ does not leak then $P_{X,Y}$ is a trivial primitive.*

Proof. Theorem 4.5 implies that if there is a 0-leaking embedding of $P_{X,Y}$ then there is also a 0-leaking embedding of $P_{X \searrow Y, Y \searrow X}$. Let us therefore assume that $|\psi\rangle$ is a non-leaking embedding of $P_{X,Y}$ such that $X \equiv X \searrow Y$ and $Y \equiv Y \searrow X$. We can write $|\psi\rangle$ in the form $|\psi\rangle = \sum_x \sqrt{P_X(x)} |x\rangle |\varphi_x\rangle$ and get $\rho_B = \sum_x P_X(x) |\varphi_x\rangle \langle \varphi_x|$. For the leakage of $|\psi\rangle$ we have: $\Delta_\psi(P_{X,Y}) = S(X; B) - I(X; Y) = S(\rho_B) - I(X; Y) = 0$. From the Holevo bound (Theorem 2.2) follows that the states $\{|\varphi_x\rangle\}_x$ form an orthonormal basis of their span (since $X \equiv X \searrow Y$, they are all different) and that Y captures the result of a measurement in this basis, which therefore is the computational basis. Since $Y \equiv Y \searrow X$, we get that for each x , there is a single $y_x \in \mathcal{Y}$ such that $|\varphi_x\rangle = |y_x\rangle$. Primitives $P_{X \searrow Y, Y \searrow X}$ and $P_{X,Y}$ are therefore trivial. \square

In other words, the only primitives that two-party quantum protocols can implement strict-correctly (without the help of a trusted third party) without leakage are the trivial ones! We note also that strict correctness is not required for Theorem 4.6 to be true. A slightly more involved proof can be done solely based on the correct distribution of the output values. This result can be seen as a quantum extension of the corresponding characterization for the cryptographic power of classical protocols in the HBC model. *Whereas classical two-party protocols cannot achieve anything non-trivial, their quantum counterparts necessarily leak information when they implement non-trivial primitives.*

4.3 Tripartite Embeddings

In this section, we extend the notion of leakage to protocols involving a trusted third party. A special case of such protocols are the ones where the players are allowed one call to a black box who provides them with classical variables \tilde{X}, \tilde{Y} sampled according to distribution $P_{\tilde{X}, \tilde{Y}}$. It is natural to ask which primitives $P_{X,Y}$ can be implemented without leakage in this case.

The state produced by purifying Alice's and Bob's actions in such a protocol up to the final measurement yielding X and Y can without loss of generality be viewed as a pure state shared among Alice, Bob and an environment $|\psi\rangle_{EABAB'} = \sum_e \sqrt{P_E(e)} |e\rangle_E \otimes |\psi^e\rangle_{ABAB'}$. We define tripartite embeddings of a primitive $P_{X,Y}$ analogously to the case of embeddings:

Definition 4.7. A state $|\psi\rangle = \sum_e P_E(e) |e\rangle_E \otimes |\psi^e\rangle_{ABAB'}$ is a tripartite embedding of $P_{X,Y}$, if measuring registers A and B in the computational basis yields X, Y with distribution $P_{X,Y}$ and the ensemble $\rho_{ABAB'} := \text{tr}_E |\psi\rangle \langle \psi|$ satisfies $S(X; YB') = S(XA'; Y) = I(X; Y)$.

The generalization of the notion of leakage to tripartite embeddings is straightforward:

Definition 4.8. Let $|\psi\rangle \in \mathcal{H}_E \otimes \mathcal{H}_{ABAB'}$ be a tripartite embedding of $P_{X,Y}$. We define the leakage of $\rho_{ABAB'} := \text{tr}_E |\psi\rangle \langle \psi|$ viewed as an implementation of $P_{X,Y}$ as

$$\Delta_{\rho_{ABAB'}}(P_{X,Y}) := \max \{S(X; BB') - I(X; Y), S(AA'; Y) - I(X; Y)\}.$$

The leakage of a tripartite embedding is non-negative, for the same reason as in the bipartite case. However, it is not necessarily symmetric, for instance for the state $|\psi\rangle_{EAB} = \sqrt{1/3}(|001\rangle + |110\rangle + |111\rangle)$ which can be verified numerically.

The following theorem shows that non-leaking embeddings of any given primitive have the property that Bob's register \tilde{B} holding his dependent part $Y \searrow X$ has to be classical if Alice honestly measures her register A in the computational basis to obtain X . An analogous statement holds with the roles of Alice and Bob exchanged. Intuitively, this means that Bob cannot learn more than $Y \searrow X$ about Alice's outcome X from a non-leaking embedding.

Theorem 4.9. Let $|\psi\rangle \in \mathcal{H}_E \otimes \mathcal{H}_{ABA'B'}$ be a non-leaking tripartite embedding of primitive $P_{X,Y}$, where $\mathcal{H}_A = \mathcal{H}_{\tilde{A}} \otimes \mathcal{H}_{\tilde{A}^\perp}$ and $\mathcal{H}_B = \mathcal{H}_{\tilde{B}} \otimes \mathcal{H}_{\tilde{B}^\perp}$. Then, there exist unitary transforms $U \in \mathcal{U}(A)$ and $V \in \mathcal{U}(B)$ such that the state $|\psi_{U,V}\rangle = (U \otimes \mathbb{I}_{A'} \otimes V \otimes \mathbb{I}_{B'})|\psi\rangle$ has the following property. Let $\tilde{\rho}_{X\tilde{B}\tilde{B}^\perp B'}$ and $\tilde{\rho}_{\tilde{A}Y\tilde{A}^\perp A'}$ be the states obtained when register A of $\text{tr}_{EA'}(|\psi_{U,V}\rangle\langle\psi_{U,V}|)$ is measured in the computational basis to obtain X , and register B of $\text{tr}_{EB'}(|\psi_{U,V}\rangle\langle\psi_{U,V}|)$ is measured in the computational basis to obtain Y . It then holds that

$$\tilde{\rho}_{X\tilde{B}\tilde{B}^\perp B'} = \sum_{x,\tilde{y}} P_{X,Y \searrow X}(x,\tilde{y}) |x\rangle\langle x|_X \otimes |\tilde{y}\rangle\langle\tilde{y}|_{\tilde{B}} \otimes \sigma_{\tilde{B}^\perp B'}^{\tilde{y}}$$

and

$$\tilde{\rho}_{\tilde{A}Y\tilde{A}^\perp A'} = \sum_{\tilde{x},y} P_{X \searrow Y,Y}(\tilde{x},y) |\tilde{x}\rangle\langle\tilde{x}|_{\tilde{A}} \otimes |y\rangle\langle y|_Y \otimes \tau_{\tilde{A}^\perp A'}^{\tilde{x}},$$

for some set of density matrices $\{\sigma^{\tilde{y}}\}_{\tilde{y}}$ in $\mathcal{H}_{\tilde{B}^\perp B'}$ and $\{\tau^{\tilde{x}}\}_{\tilde{x}}$ in $\mathcal{H}_{\tilde{A}^\perp A'}$.

Proof. Let $|\psi\rangle_{EABA'B'}$ be a tripartite embedding of $P_{X,Y}$:

$$|\psi\rangle = \sum_{e,x,y,i,j} \sqrt{P_{E,X,Y,I,J}(e,x,y,i,j)} e^{i\theta(e,x,y,i,j)} |e,x,y,i,j\rangle_{EABA'B'}.$$

Let U and V be unitary transforms acting in \mathcal{H}_A and \mathcal{H}_B respectively and extracting each party's dependent part ($X \searrow Y$ and $Y \searrow X$ respectively) in subregisters $\tilde{A} \subseteq A$ and $\tilde{B} \subseteq B$ respectively:

$$U|x\rangle_A = |f(x)\rangle_{\tilde{A}} \otimes |\mu_x\rangle_{\tilde{A}^\perp} \text{ and } V|y\rangle_B = |g(y)\rangle_{\tilde{B}} \otimes |\nu_y\rangle_{\tilde{B}^\perp},$$

for classical functions f and g providing the dependent parts $X \searrow Y$ and $Y \searrow X$ associated to X and Y respectively. For U and V to be unitary, we have that $\langle\mu_x|\mu_{x'}\rangle = 0$ for all $x \neq x'$ such that $f(x) = f(x')$, and that $\langle\nu_y|\nu_{y'}\rangle = 0$ for all $y \neq y'$ such that $g(y) = g(y')$. We define

$$\begin{aligned} |\tilde{\psi}\rangle &= (\mathbb{I}_E \otimes U \otimes \mathbb{I}_{A'} \otimes V \otimes \mathbb{I}_{B'})|\psi\rangle \\ &= \sum_{e,x,y,i,j} \sqrt{P_{E,X,Y,I,J}(e,x,y,i,j)} e^{i\theta(e,x,y,i,j)} |e,f(x),g(y)\rangle_{\tilde{A}\tilde{B}} \otimes \\ &\quad |\mu_x\rangle_{\tilde{A}^\perp} |\nu_y\rangle_{\tilde{B}^\perp} |i,j\rangle_{A'B'}, \end{aligned}$$

where $\mathcal{H}_{\tilde{A}\tilde{A}^\perp} \cong \mathcal{H}_A$ and $\mathcal{H}_{\tilde{B}\tilde{B}^\perp} \cong \mathcal{H}_B$. Re-writing $|\tilde{\psi}\rangle$ in terms of the different values which X may take results in:

$$\begin{aligned} |\tilde{\psi}\rangle &= \sum_x \sqrt{P_X(x)} |x\rangle_A \otimes \sum_{e,i} \sqrt{P_{E,I|X=x}(e,i)} |e,i\rangle_{EA'} |\varphi_{e,x,i}\rangle_{BB'} \\ &=: \sum_x \sqrt{P_X(x)} |x\rangle_A \otimes |\zeta_x\rangle_{A'E\tilde{B}\tilde{B}^\perp B'}. \end{aligned}$$

We can view the information provided to Bob about X as the information available about X when encoded by $x \mapsto \rho_x$ where:

$$\rho_x = \text{tr}_{A'E}(|\zeta_x\rangle\langle\zeta_x|) = \sum_{e,i} P_{E,I|X=x}(e,i) |\varphi_{e,i}\rangle\langle\varphi_{e,i}|_{BB'}.$$

By basic properties of the von Neumann entropy, we have that

$$\begin{aligned}
S(X; BB')_\psi &= S(X; BB')_{\tilde{\psi}} \\
&= S(X; \tilde{B} \tilde{B}^\perp B')_{\tilde{\psi}} \\
&\geq S(X; Y \searrow X \tilde{B}^\perp B')_{\tilde{\psi}} \\
&\geq I(X; Y \searrow X) .
\end{aligned}$$

Suppose now that $|\psi\rangle$ is non-leaking, that is $S(X; BB') = I(X; Y) = I(X; Y \searrow X)$. It follows that for non-leaking embeddings, all terms above are actually equal.

By the Holevo bound (Theorem 2.2), we conclude that states in $\{\rho_x\}_x$ are simultaneously diagonalizable. In other words, for all x ,

$$\rho_x = \sum_z P_{Z|X=x}(z) |\gamma_z\rangle\langle\gamma_z|_{BB'} ,$$

where $\{|\gamma_z\rangle\}_z$ form an orthonormal basis for some subspace of $\mathcal{H}_{\tilde{B} \tilde{B}^\perp B'}$. Since $S(X; BB')_{\tilde{\psi}} = S(X; Y \searrow X \tilde{B}^\perp B')_{\tilde{\psi}}$, we conclude that such a basis can be chosen to be the computational basis for the register \tilde{B} holding $Y \searrow X$:

$$\begin{aligned}
\tilde{\rho}_{X \tilde{B} \tilde{B}^\perp B'} &= \sum_x P_X(x) |x\rangle\langle x|_X \otimes \rho_x \\
&= \sum_x P_X(x) |x\rangle\langle x|_X \otimes \sum_z P_{Z|X=x}(z) |\gamma_z\rangle\langle\gamma_z|_{BB'} \\
&= \sum_x P_X(x) |x\rangle\langle x|_X \otimes \sum_{\tilde{y}} P_{Y \searrow X|X=x}(\tilde{y}) |\tilde{y}\rangle\langle\tilde{y}|_{\tilde{B}} \otimes \sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x} \\
&= \sum_{x, \tilde{y}} P_{X, Y \searrow X}(x, \tilde{y}) |x\rangle\langle x|_X \otimes |\tilde{y}\rangle\langle\tilde{y}|_{\tilde{B}} \otimes \sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x} .
\end{aligned}$$

We now observe that $|\psi\rangle$ being non-leaking implies that $\sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x}$ cannot depend on x . Otherwise, suppose that for some \tilde{y} there exist $x \neq x'$ such that $\sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x} \neq \sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x'}$ with $P_{X, Y \searrow X}(x, \tilde{y}) > 0$ and $P_{X, Y \searrow X}(x', \tilde{y}) > 0$. After having measured \tilde{y} , Bob can apply an optimal measurement for distinguishing between $\sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x}$ and $\sigma_{\tilde{B}^\perp B'}^{\tilde{y}, x'}$ with some strictly positive bias allowing him to get more information than $I(X; Y \searrow X)$ thereby implying that $|\psi\rangle$ is leaking. It follows that

$$\tilde{\rho}_{X \tilde{B} \tilde{B}^\perp B'} = \sum_{x, \tilde{y}} P_{X, Y \searrow X}(x, \tilde{y}) |x\rangle\langle x|_X \otimes |\tilde{y}\rangle\langle\tilde{y}|_{\tilde{B}} \otimes \sigma_{\tilde{B}^\perp B'}^{\tilde{y}} .$$

The same argument symmetrically applied to $\rho_{\tilde{A} Y \tilde{A}^\perp A'}$ leads to

$$\tilde{\rho}_{\tilde{A} Y \tilde{A}^\perp A'} = \sum_{\tilde{x}, y} P_{X \searrow Y, Y}(\tilde{x}, y) |\tilde{x}\rangle\langle\tilde{x}|_{\tilde{A}} \otimes |y\rangle\langle y|_Y \otimes \tau_{\tilde{A}^\perp A'}^y .$$

□

For the remainder of this section, we focus on primitives $P_{X, Y}$ where each variable is equivalent to its dependent part: $X \equiv X \searrow Y$ and $Y \equiv Y \searrow X$. For non-leaking tripartite embeddings of these primitives, we establish lower bounds on the conditional von Neumann entropy of the environment given each party's quantum states.

In order to define what we mean by the entropy of the environment, we decompose any tripartite embedding $|\psi\rangle$ of $P_{X,Y}$ in its Schmidt form with respect to the environment:

$$|\psi\rangle_{EABAB'} = \sum_w \sqrt{\lambda_w} |e_w\rangle_E \otimes |\psi_w\rangle_{ABAB'} ,$$

where $\langle e_w | e_{w'} \rangle = \langle \psi_w | \psi_{w'} \rangle = \delta_{w,w'}$. Now, imagine the environment measures register E in the Schmidt basis $\{|e_w\rangle\}_w$ to get classical random outcome W such that $\Pr[W = w] = \lambda_w$. Corollary 4.10 below shows that non-leaking tripartite embeddings of $P_{X,Y}$ must satisfy $S(W|AA') \geq H(Y|X)$ and $S(W|BB') \geq H(X|Y)$. If the Schmidt decomposition is not unique, the result holds for a measurement in any Schmidt basis. Measurements in the Schmidt basis minimize the entropy of the outcome among any complete Von Neumann measurement applied to the state of the environment. Intuitively, $S(W|AA')$ measures the amount of *shared entanglement* between Alice and the environment (similarly, $S(W|BB')$ is a measure for the shared entanglement between Bob and the environment). The more non-trivial a primitive gets, the more the environment has to be entangled with the players in order to preserve privacy.

Corollary 4.10. *Let $|\psi\rangle_{EABAB'}$ be any non-leaking tripartite embedding of $P_{X,Y}$ where $X \equiv X \searrow Y$ and $Y \equiv Y \searrow X$. Let W be the random variable for the outcome of measuring the environment register E in a Schmidt basis. Then,*

$$\begin{aligned} S(W|AA') &= S(W|X A') \geq H(Y|X) = H(Y \searrow X | X \searrow Y) \text{ and} \\ S(W|BB') &= S(W|Y B') \geq H(X|Y) = H(X \searrow Y | Y \searrow X) . \end{aligned}$$

Proof. Let us write the non-leaking tripartite embedding as a function of Alice's output $X = x$ as follows

$$|\psi\rangle_{ABEAB'} = \sum_x \sqrt{P_X(x)} |x\rangle_A \otimes \sum_y \sqrt{P_{Y|X=x}(y)} |y\rangle_B \otimes \sum_a \kappa_a^{x,y} |a\rangle_{A'} \otimes |\mu^{x,y,a}\rangle_{EB'} , \quad (12)$$

where we assume without loss of generality that all $\kappa_a^{x,y}$ are real (and possible complex phases are put into $|\mu^{x,y,a}\rangle$). We claim that $\kappa_a^{x,y} = \kappa_a^x$, i.e. the coefficients do not depend on y . To see this, let $p_a^x = \Pr(A' = a | X = x)$ where A' denotes the classical outcome of measuring register A' in the computational basis. Suppose for a contradiction that there exists y such that $|\kappa_a^{x,y}|^2 \neq p_a^x$:

$$\begin{aligned} \Pr(Y = y | X = x, A' = a) &= \frac{\Pr(Y = y | X = x) \Pr(A' = a | X = x, Y = y)}{\Pr(A' = a | X = x)} \\ &= \frac{\Pr(Y = y | X = x) |\kappa_a^{x,y}|^2}{p_a^x} \\ &\neq \Pr(Y = y | X = x) , \end{aligned}$$

which would contradict the fact that $|\psi\rangle$ is non-leaking. Hence, we can write $|\psi\rangle$ as

$$|\psi\rangle_{ABEAB'} = \sum_x \sqrt{P_X(x)} |x\rangle_A \sum_a \kappa_a^x |a\rangle_{A'} |\eta^{x,a}\rangle_{BEB'} ,$$

where

$$\begin{aligned} |\eta^{x,a}\rangle_{BEB'} &= \sum_y \sqrt{P_{Y|X=x}(y)} |y\rangle_B |\mu^{x,y,a}\rangle \\ &= \sum_y \sqrt{P_{Y|X=x}(y)} |y\rangle_B \sum_i \sqrt{\lambda_i^{x,y,a}} |e_i^{x,y,a}\rangle_E \otimes |b_i^{x,y,a}\rangle_{B'} , \end{aligned}$$

where in the last step, we wrote the bipartite states $|\mu^{x,y,a}\rangle_{EB'}$ in the Schmidt form.

Theorem 4.9 establishes that if $|\psi\rangle$ is non-leaking then

$$\text{tr}_E (|\eta^{x,a}\rangle\langle\eta^{x,a}|_{BEB'}) = \sum_y P_{Y|X=x}(y) |y\rangle\langle y|_B \otimes \sigma_{B'}^y . \quad (13)$$

We claim that (13) implies that the subspaces $S_a^{x,y} = \text{span}_i\{|e_i^{x,y,a}\rangle_E\}$ must be perpendicular for different values of y . Let $q_y^x := \sqrt{P_{Y|X=x}(y)}$ be used to shorten the notation. We have

$$\begin{aligned} \text{tr}_E (|\eta^{x,a}\rangle\langle\eta^{x,a}|_{BEB'}) &= \sum_{y,y'} q_y^x q_{y'}^x \text{tr}_E \left(|y\rangle\langle y'|_B \otimes |\mu^{x,y,a}\rangle\langle\mu^{x,y',a}|_{EB'} \right) \\ &= \sum_{y,y'} q_y^x q_{y'}^x \text{tr}_E \left(|y\rangle\langle y'|_B \otimes \sum_{i,j} |e_i^{x,y,a}\rangle\langle e_j^{x,y',a}|_E \otimes |b_i^{x,y,a}\rangle\langle b_j^{x,y',a}|_{B'} \right) \\ &= \sum_{y,y'} q_y^x q_{y'}^x |y\rangle\langle y'|_B \otimes \text{tr}_E \left(\sum_{i,j} |e_i^{x,y,a}\rangle\langle e_j^{x,y',a}|_E \otimes |b_i^{x,y,a}\rangle\langle b_j^{x,y',a}|_{B'} \right) \\ &= \sum_{y,y'} q_y^x q_{y'}^x |y\rangle\langle y'|_B \otimes \\ &\quad \sum_h \langle e_h^{x,y,a} | \left(\sum_{i,j} |e_i^{x,y,a}\rangle\langle e_j^{x,y',a}|_E \otimes |b_i^{x,y,a}\rangle\langle b_j^{x,y',a}|_{B'} \right) | e_h^{x,y,a} \rangle \\ &= \sum_{y,y'} q_y^x q_{y'}^x |y\rangle\langle y'|_B \otimes \sum_{i,j} \langle e_j^{x,y',a} | e_i^{x,y,a} \rangle \otimes |b_i^{x,y,a}\rangle\langle b_j^{x,y',a}|_{B'} . \quad (14) \end{aligned}$$

Clearly, if $S_a^{x,y} \perp S_a^{x,y'}$ is not satisfied then there exists $i \neq j, y \neq y'$ such that $\langle e_j^{x,y',a} | e_i^{x,y,a} \rangle \neq 0$ and register B is not diagonal in the computational basis according (14).

It follows that for $X = x$, any $A' = a$, and when $Y = y$ is measured by Bob, the environment E ends up in subspace $S_a^{x,y}$ of E which corresponds to $Y = y$ unambiguously. As W is the outcome of measuring E in the Schmidt basis, knowledge of W , X and A' determines Y . Formally, we have $0 \leq S(Y|WXA') \leq S(Y|WXA') = 0$ and it follows that

$$\begin{aligned} S(W|XA') &= S(W|XA') + S(Y|WXA') \\ &= S(WY|XA') \\ &\geq S(Y|XA') \\ &= H(Y|X) , \end{aligned} \quad (15)$$

where the inequality holds due to the classicality of W and the last step is due to strict correctness.

The same argument with the roles of Alice and Bob reversed results in:

$$S(W|Y B') \geq H(X|Y) . \quad (16)$$

Equations (15) and (16) establish the inequalities of the statement.

To prove the statement's equalities, consider Theorem 4.9 when Bob measures Y :

$$\tilde{\rho}_{A'AY} = \sum_{x,y} P_{X,Y}(x,y) \tau_{A'}^x \otimes |x,y\rangle\langle x,y|_{AY} ,$$

which obviously means that

$$\tilde{\rho}_{A'A} = \sum_x P_X(x) \tau_{A'}^x \otimes |x\rangle\langle x|_A .$$

Alice's register A is therefore diagonal in the computational basis. It follows that

$$S(W|A A') = S(W|X A') .$$

A symmetric argument from (16) shows that

$$S(W|B B') = S(W|Y B') .$$

□

Suppose Alice and Bob have access to an ideal functionality for $P_{X,Y}$ as a cryptographic resource. What primitives can Alice and Bob implement without leakage given access to this resource? Is it possible for them to “promote” the ideal functionality for $P_{X,Y}$ to a stronger cryptographic primitive? Before answering this question in the negative, let us define what we exactly mean by an *ideal functionality* for primitive $P_{X,Y}$:

Definition 4.11. *An ideal functionality $\text{ID}(P_{X,Y})$ for primitive $P_{X,Y}$ is a box that provides Alice and Bob with X and Y respectively and nothing more. In particular, the ideal functionality never provides extra working registers (otherwise, extra registers could without violating strict correctness provide additional cryptographic resources to Alice and Bob). More formally,*

$$\text{ID}(P_{X,Y}) = \sum_{x,y} P_{X,Y}(x,y) |x\rangle\langle x|_A \otimes |y\rangle\langle y|_B .$$

The next theorem shows that one call to an ideal functionality is never sufficient for a non-leaking implementation of a stronger primitive. In other words, quantum communication and computation never allow to amplify an ideal classical two-party cryptographic primitive into a stronger one without leakage.

Theorem 4.12. *Let $P_{X,Y}$ and $P_{X',Y'}$ be two primitives, where $X \equiv X \searrow Y$, $Y \equiv Y \searrow X$, $X' \equiv X' \searrow Y'$, and $Y' \equiv Y' \searrow X'$. Suppose that $H(X'|Y') > H(X|Y)$ or $H(Y'|X') > H(Y|X)$. Then, any implementation of $P_{X',Y'}$ using just one call to the ideal functionality $\text{ID}(P_{X,Y})$ leaks information.*

Proof. We may view the ideal functionality $\text{ID}(P_{X,Y})$ as a box that conceals its environment to Alice and Bob. For instance, the state

$$|\psi\rangle_{E\hat{A}\hat{B}} = \sum_{x,y} \sqrt{P_{X \searrow Y, Y \searrow X}(x,y)} |x,y\rangle_E \otimes |x,y\rangle_{\hat{A}\hat{B}} .$$

is a non-leaking embedding of $P_{X \searrow Y, Y \searrow X}$ with $S(W|\hat{A}) = H(Y|X)$ and $S(W|\hat{B}) = H(X|Y)$ where W is defined as above as the classical outcome when measuring the environment in the Schmidt basis.

Consider any strictly correct protocol implementing $P_{X',Y'}$ where Alice and Bob purify their actions but are otherwise honest. An execution of the protocol will produce a non-leaking tripartite embedding of $P_{X',Y'}$. Just before the call to $\text{ID}(P_{X,Y})$, Alice's internal register A_0 and Bob's internal register B_0 are such that

$$S(W|A_0) = S(W|B_0) = 0 \quad ,$$

since the environment is in a pure state. Just after the call to $\text{ID}(P_{X,Y})$, Alice's register A_1 and Bob's register B_1 satisfy:

$$S(W|A_1) = H(Y|X) \text{ and } S(W|B_1) = H(X|Y) \quad ,$$

since $\hat{A} \subseteq A_1$ and $\hat{B} \subseteq B_1$. Notice also that the state provided to Alice and Bob by $\text{ID}(P_{X,Y})$ is diagonal in the computational basis: the information is classical. It follows that Alice and Bob can copy this information and keep it with them during the execution of the protocol while remaining able to run the protocol in a honest-but-curious fashion. The Schmidt basis for the environment remains the same after the call to $\text{ID}(P_{X,Y})$. It follows that at any point t in the protocol evolution, Alice's and Bob's internal quantum registers A_t and B_t respectively are such that:

$$S(W|A_t) \leq H(Y|X) \text{ and } S(W|B_t) \leq H(X|Y) \quad . \quad (17)$$

That is, $S(W|A_t)$ and $S(W|B_t)$ are non-increasing monotones for honest-but-curious quantum players in secure two-party computation similar to $H(Y|X)$ and $H(X|Y)$ in the classical case [WW04].

At the very last step t_{\max} of the protocol, $A_{t_{\max}} := A \otimes A'$ and $B_{t_{\max}} := B \otimes B'$. Therefore,

$$S(W|A A') \leq H(Y|X) \text{ and } S(W|B B') \leq H(X|Y) \quad .$$

Since $H(Y|X) < H(Y'|X')$ or $H(X|Y) < H(X'|Y')$, we conclude that either $S(W|A A') < H(Y'|X')$ or $S(W|B B') < H(X'|Y')$. It follows by Corollary 4.10 that the implementation of $P_{X',Y'}$ must leak. \square

As in the classical case [WW04], it is straightforward to use Theorem 4.12 in order to determine a lower bound on the number of calls to a weaker primitive required to implement a stronger one without leakage: $P_{X',Y'}$ can be implemented without leakage by n calls to $P_{X,Y}$ only if $H(X'|Y') \leq nH(X|Y)$ and $H(Y'|X') \leq nH(Y|X)$.

4.4 Reducibility of Primitives and Their Leakage

This section is concerned with the following question: Given two primitives $P_{X,Y}$ and $P_{\tilde{X},\tilde{Y}}$ such that $P_{X,Y}$ is reducible to $P_{\tilde{X},\tilde{Y}}$, what is the relationship between the leakage of $P_{X,Y}$ and the leakage of $P_{\tilde{X},\tilde{Y}}$? We use the notion of reducibility in the following sense: We say that a primitive $P_{X,Y}$ is *reducible in the HBC model* to a primitive $P_{\tilde{X},\tilde{Y}}$ if $P_{X,Y}$ can be securely implemented in the HBC model from (one call to) a secure implementation of $P_{\tilde{X},\tilde{Y}}$. The above question can also be generalized to the case where $P_{X,Y}$ can be computed from $P_{\tilde{X},\tilde{Y}}$ only with certain probability. Notice that the answer, even if we assume perfect reducibility, is not captured in our previous result from Lemma 4.3, since an embedding of $P_{\tilde{X},\tilde{Y}}$ is not necessarily an embedding of $P_{X,Y}$ (it might violate the strict correctness condition). However, under certain circumstances, we can show that $\Delta_{P_{\tilde{X},\tilde{Y}}} \geq \Delta_{P_{X,Y}}$.

Theorem 4.13. Assume that primitives $P_{X,Y}$ and $P_{\tilde{X},\tilde{Y}} = P_{\tilde{X}_0\tilde{X}_1,\tilde{Y}_0\tilde{Y}_1}$ satisfy the condition:

$$\sum_{x,y:P_{\tilde{X}_0,\tilde{Y}_0|\tilde{X}_1=x,\tilde{Y}_1=y} \simeq P_{X,Y}} P_{\tilde{X}_1,\tilde{Y}_1}(x,y) \geq 1 - \delta,$$

where the relation \simeq means that the two distributions are equal up to relabeling of the alphabet. Then, $\Delta_{P_{\tilde{X},\tilde{Y}}} \geq (1 - \delta)\Delta_{P_{X,Y}}$.

Proof. State $|\psi\rangle_{A_0A_1B_0B_1} \in \mathcal{E}(P_{\tilde{X},\tilde{Y}})$ can be written in the form:

$$|\psi\rangle = \sum_{x \in \mathcal{X}'_1} \sqrt{P_{\tilde{X}_1}(x)} |x\rangle_{A_1} |\psi^x\rangle_{A_0B},$$

where each $|\psi^x\rangle$ is a regular embedding of $P_{\tilde{X}_0\tilde{Y}_0\tilde{Y}_1|\tilde{X}_1=x}$. Due to the Holevo bound (Theorem 2.2), we have

$$S(\tilde{Y}|A)_\psi = S(\tilde{Y}|A_0A_1)_\psi \leq S(\tilde{Y}|A_0, \tilde{X}_1)_\psi = \sum_x P_{\tilde{X}_1}(x) S(\tilde{Y}|A_0, \tilde{X}_1 = x)_{\psi^x},$$

and we obtain for the leakage of $|\psi\rangle$ that

$$\begin{aligned} \Delta_\psi(P_{\tilde{X},\tilde{Y}}) &= H(\tilde{Y}|\tilde{X}) - S(\tilde{Y}|A)_\psi \\ &\geq H(\tilde{Y}|\tilde{X}) - \sum_x P_{\tilde{X}_1}(x) S(\tilde{Y}|A_0, \tilde{X}_1 = x)_{\psi^x} \\ &= \sum_x P_{\tilde{X}_1}(x) (H(\tilde{Y}|\tilde{X}_0, \tilde{X}_1 = x) - S(\tilde{Y}|A_0, \tilde{X}_1 = x)_{\psi^x}) \\ &= \sum_x P_{\tilde{X}_1}(x) \Delta_{\psi^x}(P_{\tilde{X}_0,\tilde{Y}_0\tilde{Y}_1|\tilde{X}_1=x}). \end{aligned}$$

By applying the same argument to each $|\psi^x\rangle$, we obtain that

$$\Delta_\psi(P_{\tilde{X},\tilde{Y}}) \geq \sum_{xy} P_{\tilde{X}_1,\tilde{Y}_1}(x,y) \Delta_{\psi^{x,y}}(P_{\tilde{X}_0,\tilde{Y}_0|\tilde{X}_1=x,\tilde{Y}_1=y}), \quad (18)$$

where each $|\psi^{x,y}\rangle$ is a regular embedding of $P_{\tilde{X}_0,\tilde{Y}_0|\tilde{X}_1=x,\tilde{Y}_1=y}$. For each (x,y) such that $P_{\tilde{X}_0,\tilde{Y}_0|\tilde{X}_1=x,\tilde{Y}_1=y} \simeq P_{X,Y}$ is satisfied, we get that

$$\Delta_{\psi^{x,y}}(P_{\tilde{X}_0,\tilde{Y}_0|\tilde{X}_1=x,\tilde{Y}_1=y}) \geq \Delta_{P_{X,Y}}.$$

Since $\sum_{x,y:P_{\tilde{X}_0,\tilde{Y}_0|\tilde{X}_1=x,\tilde{Y}_1=y} \simeq P_{X,Y}} P_{\tilde{X}_1,\tilde{Y}_1}(x,y) \geq 1 - \delta$, we get from (18) that

$$\Delta_\psi(P_{\tilde{X},\tilde{Y}}) \geq (1 - \delta)\Delta_{P_{X,Y}}.$$

□

Theorem 4.13 will allow to derive a lower bound on the leakage of 1-out-of-2 Oblivious Transfer of r -bit strings in Section 5.

5 The Leakage of Universal Cryptographic Primitives

In this section, we exhibit lower bounds on the leakage of the following universal two-party primitives.

String Rabin OT (ROT^r): [Rab81] Alice sends a random string of r bits to Bob who receives it with probability $1/2$, otherwise he receives a special symbol \perp . Alice does not learn any information about whether Bob has received the string she sent.
For $x \in \{0, 1\}^r$ and $y \in \{0, 1\}^r \cup \{\perp\}$:

$$P_{X,Y}^{\text{ROT}^r}(x, y) = \begin{cases} 2^{-r-1} & \text{if } x = y \text{ or } y = \perp, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to an execution of Rabin OT of a random binary string of length r .

One-out-of-two String OT (1-2-OT^r): [Wie83,EGL82] Alice sends two random r -bit strings to Bob who decides which of them he receives. Bob does not learn any information about the other one of Alice's strings and Alice does not learn which of the strings has been received by Bob. We simply write 1-2-OT for the case of 1-out-of-2 oblivious transfer of bits ($r = 1$).

For $x_0, x_1, y \in \{0, 1\}^r$ and $c \in \{0, 1\}$:

$$P_{X,Y}^{\text{OT}^r}((x_0, x_1), (c, y)) = \begin{cases} 2^{-2r-1} & \text{if } y = x_c, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to an execution of one-out-of-two r -bit string OT upon random inputs.

Additive sharing of AND (SAND): [PR94] Alice and Bob choose their respective input bits x and y , and receive the output bits a resp. b such that $a \oplus b = x \wedge y$ and $\Pr[a = 0] = 1/2$. They do not get any other information.

For $x, y, a, b \in \{0, 1\}$:

$$P_{X,Y}^{\text{NL}}((x, a), (y, b)) = \begin{cases} \frac{1}{8} & \text{if } xy = a \oplus b, \\ 0 & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to the generation of an additive sharing for the AND of two random bits.

Noisy one-out-of-two OT (1-2-OT_p): Alice sends two bits to Bob who decides which of them he wants to receive. The selected bit is transmitted to him over a noisy channel with noise rate p . Bob does not learn any information about the other one of Alice's bits and Alice does not learn any information about Bob's selection bit.

For $x_0, x_1, y, c \in \{0, 1\}$ and $p \in (0, 1/2)$:

$$P_{X,Y}^{\text{OT}_p}((x_0, x_1), (c, y)) = \begin{cases} \frac{1-p}{8} & \text{if } y = x_c, \\ \frac{p}{8} & \text{otherwise,} \end{cases}$$

is the joint probability distribution associated to an execution of one-out-of-two OT where the selected bit is received through a binary symmetric channel with error rate p .

primitive	leaking at least	comments
ROT^1	$(h(\frac{1}{4}) - \frac{1}{2}) \approx 0.311$	same leakage for all regular embeddings
ROT^r	$(1 - O(r2^{-r}))$	same leakage for all regular embeddings
1-2-OT, SAND	$\frac{1}{2}$	minimized by canonical embedding
1-2-OT ^r	$(1 - O(r2^{-r}))$	(suboptimal) lower bound
1-2-OT _p	$\frac{(1/2 - p - \sqrt{p(1-p)})^2}{8 \ln 2}$	if $p < \sin^2(\pi/8) \approx 0.15$, (suboptimal) lower bound

Table 1. Lower bounds on the leakage for universal two-party primitives

Table 1 summarizes the lower bounds on the leakage of these primitives (the derivations can be found in Appendix A). We note that Wolf and Wullschleger [WW05b] have shown that a randomized 1-2-OT can be transformed by local operations into an additive sharing of an AND (here called SAND). Therefore, our results for 1-2-OT below also apply to SAND.

1-2-OT^r and 1-2-OT_p are primitives where the direct evaluation of the leakage for a general embedding $|\psi_\theta\rangle$ is hard, because the number of possible phases increases exponentially in the number of qubits. Instead of computing $S(A)$ directly, we derive (suboptimal) lower bounds on the leakage.

For the primitive $P_{X,Y}^{\text{OT}_p}$, our lower bound on the leakage only holds for $p < \sin^2(\pi/8) \approx 0.15$. Notice that in reality, the leakage is strictly positive for any embedding of $P_{X,Y}^{\text{OT}_p}$ with $p < 1/4$, since for $p < 1/4$, $P_{X,Y}^{\text{OT}_p}$ is a non-trivial primitive. On the other hand, $P_{X,Y}^{\text{OT}_{1/4}}$ is a trivial primitive implemented securely by the following protocol in the classical HBC model:

1. Alice chooses randomly between her input bits x_0 and x_1 and sends the chosen value x_a to Bob.
2. Bob chooses his selection bit c uniformly at random and sets $y := x_a$.

Equality $x_c = y$ is satisfied if either $a = c$, which happens with probability $1/2$, or if $a \neq c$ and $x_a = x_{1-a}$, which happens with probability $1/4$. Since the two events are disjoint, it follows that $x_c = y$ with probability $3/4$ and that the protocol implements $P_{X,Y}^{\text{OT}_{1/4}}$. The implementation is clearly secure against honest-but-curious Alice, since she does not receive any message from Bob. It is also secure against Bob, since he receives only one bit from Alice. By letting Alice randomize the value of the bit she is sending, the players can implement $P_{X,Y}^{\text{OT}_p}$ securely for any value $1/4 < p \leq 1/2$.

6 Conclusion and Open Problems

We have provided a quantitative extension of qualitative impossibility results for two-party quantum cryptography. All non-trivial classical primitives leak information when implemented by quantum protocols. Notice that demanding a protocol to be non-leaking does in general not imply the privacy of the players' outputs. For instance, consider a protocol implementing 1-2-OT but allowing a curious receiver with probability $\frac{1}{2}$ to learn both bits simultaneously or with probability $\frac{1}{2}$ to learn nothing about them. Such a protocol for 1-2-OT would be non-leaking but nevertheless insecure. Consequently, Theorem 4.6 not only tells us that any quantum protocol implementing a non-trivial primitive must be insecure, but also that a privacy breach will reveal itself as leakage. Our framework allows to quantify the leakage of any two-party quantum protocol strict-correctly implementing a

primitive. Our impossibility results are different than common ones since they only rely on the strict correctness of the protocol, not on the perfect privacy of a protocol against one party. Moreover, the generic attack that allows to show leakage is simply implemented by purifying the parties' actions. Furthermore, we present lower bounds on the leakage of some strictly correct universal two-party primitives.

A natural open question is to find a way to identify good embeddings for a given primitive. Based on the examples of ROT^r and 1-2-OT, it is tempting to conjecture the following.

Conjecture 6.1. The leakage of any primitive $P_{X,Y}$ is minimized by its canonical embedding.

The conjecture agrees with the geometric intuition that the minimal pairwise distinguishability of quantum states in a mixture minimizes the von Neumann entropy of the mixture. However, Jozsa and Schlienz have shown that this intuition is sometimes incorrect [JS00]. In a quantum system of dimension at least three, we can have the following situation: For two sets of pure states $\{|u_i\rangle\}_{i=1}^n$ and $\{|v_i\rangle\}_{i=1}^n$ satisfying $|\langle u_i|u_j\rangle| \leq |\langle v_i|v_j\rangle|$ for all i, j , there exist probabilities p_i such that for $\rho_u := \sum_{i=1}^n p_i |u_i\rangle\langle u_i|$, $\rho_v := \sum_{i=1}^n p_i |v_i\rangle\langle v_i|$, it holds that $S(\rho_u) < S(\rho_v)$. As we can see, although each pair $|u_i\rangle, |u_j\rangle$ is more distinguishable than the corresponding pair $|v_i\rangle, |v_j\rangle$, the overall ρ_u provides us with less uncertainty than ρ_v . It follows that although for the canonical embedding $|\psi_0\rangle = \sum_y |\varphi_y\rangle|y\rangle$ of $P_{X,Y}$ the mutual overlaps $|\langle \varphi_y|\varphi_{y'}\rangle|$ are clearly maximized, it does not necessarily imply that $S(A)$ in this case is minimal over $\mathcal{E}(P_{X,Y})$. It is an interesting open question to find a primitive whose canonical embedding does not minimize the leakage or to prove that no such primitive exists. In particular, how far can the leakage of the canonical embedding be from the best one? Such a characterization, even if only applicable to special primitives, would allow to lower bound their leakage and would also help to understand the power of two-party quantum cryptography in a more concise way.

A very natural generalization of our approach would be to see what happens when *strict correctness* is relaxed.

Conjecture 6.2. Any correct protocol for $P_{X,Y}$ leaks as much as a strictly correct protocol for $P_{X,Y}$.

The most obvious relaxation would be to consider as correct any $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$ that produces (x, y) with probability $P_{X,Y}(x, y)$ when registers A and B are measured but registers A' and B' can provide extra information about Y and X respectively. Remember that this is equivalent to allowing for the quantum Markov chain conditions $A' \leftrightarrow X \leftrightarrow Y$ and $B' \leftrightarrow Y \leftrightarrow X$ not to hold anymore. Would it be possible to find such a $|\psi\rangle$ with the property that for any regular embedding $|\phi\rangle \in \mathcal{E}(P_{X,Y})$:

$$\Delta_\psi(P_{X,Y}) < \Delta_\phi(P_{X,Y}) ?$$

A positive answer would reveal that some primitive $P_{X,Y}$ may be implemented with minimum leakage when viewed as a marginal in some *larger* probability distribution $P_{XX',YY'}$. A negative answer would rather show that all our results hold unaffected for the standard notion of correctness. Note however that the leakage is no more symmetric for the standard notion of correctness.

It would also be interesting to find a measure of cryptographic non-triviality for two-party primitives and see how it relates to the minimum leakage of any implementation by quantum protocols. For instance, is it true that quantum protocols for primitive $P_{X,Y}$ leak more if the *distance* between $P_{X,Y}$ and any trivial primitive increases?

Another question we leave for future research is to define and investigate other notions of leakage, e.g. in the one-shot setting instead of in the asymptotic regime (as outlined in Footnote 13). Results in the one-shot setting have already been established for data compression [RW05], channel capacities [RWW06], state-merging [WR07,Ber08] and other (quantum-) information-theoretic tasks.

Furthermore, it would be interesting to find more applications for the concept of leakage, considered also for protocols using an environment as a trusted third party. In this direction, we have shown in Theorem 4.12 that any two-party quantum protocol for a given primitive, using a black box for an “easier” primitive, leaks information. Lower-bounding this leakage is an interesting open question. We might also ask how many copies of the “easier” primitive are needed to implement the “harder” primitive by a quantum protocol, which would give us an alternative measure of non-triviality for two-party primitives.

The approach used in this paper cannot easily be applied to cryptographic primitives modeled by unitary transforms. Our approach is specialized to deal with classical primitives. It is an open question to determine the leakage of protocols implementing some unitary primitive. The few impossibility proofs for unitary primitives that we are aware of simply establish that perfect privacy cannot be achieved. For example, it is shown in [DNS10] that quantum SWAP is impossible (in fact, any unitary that never allows any of the party to recover their input state). It would be very interesting to investigate the landscape of possibilities and impossibilities for unitary primitives and see how it relates to the one for classical primitives. These two worlds might be very different¹⁷.

Acknowledgements

We would like to thank an anonymous referee for pointing out several shortcomings in earlier versions of this paper. LS is supported by the Danish Natural Science Research Council project QUSEP, and Canada’s NSERC discovery grant. CS is supported by a NWO VENI project.

References

- AKSW07. Giacomo Mauro D’ Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 76(3):032328, 2007.
- Amb05. Andris Ambainis. personal communication, 2005.
- BB84. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.
- BCH⁺08. H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner. Possibility, impossibility and cheat-sensitivity of quantum bit string commitments. *Physical Review A*, 78:022316, 2008.
- BCS12. Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters*, 109:160501, 2012.
- Ber08. Mario Berta. Single-shot quantum state merging. Master’s thesis, ETH Zurich, 2008.

¹⁷ See [FKS⁺13] for a recent classification result for quantum protocols of classical cryptographic primitives.

- BLM⁺05. Jonathan Barrett, Noah Linden, Serge Massar, Stefan Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Physical Review A*, 71:022101, 2005.
- CK91. Benny Chor and Eyal Kushilevitz. A zero-one law for boolean privacy. *SIAM J. Discrete Math.*, 4(1):36–47, 1991.
- CK09. Andre Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2009.
- CKS13. André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. *Quantum Information & Computation*, 13(1-2):158–177, 2013.
- Col07. Roger Colbeck. Impossibility of secure two-party classical computation. *Physical Review A*, 76(6):062308, 2007.
- CT91. T.M. Cover and J.A. Thomas. *Elements of Information Theory*. Wiley, 1991.
- DFSS07. Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Advances in Cryptology—CRYPTO ’07*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer, 2007.
- DNS10. Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *Advances in Cryptology—CRYPTO ’10*, volume 6223 of *Lecture Notes in Computer Science*, pages 685–706. Springer, 2010.
- EGL82. Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In *Advances in Cryptology: Proceedings of CRYPTO 82*. Plenum Press, 1982.
- FKS⁺13. Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. Feasibility and completeness of cryptographic tasks in the quantum world. In *Theory of Cryptography Conference (TCC)*, volume 7785 of *Lecture Notes in Computer Science*, pages 281–296. Springer, 2013.
- FS09. Serge Fehr and Christian Schaffner. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference (TCC)*, volume 5444 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2009.
- FWW04. Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger. Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In *Advances in Cryptology—CRYPTO ’04*, volume 3152 of *Lecture Notes in Computer Science*, pages 562–579. Springer, 2004.
- Hol73. A. S. Holevo. Information-theoretical aspects of quantum measurement. *Problemy Peredači Informacii*, 9(2):31–42, 1973.
- IMNW04. Hideki Imai, Jörn Müller-Quade, Anderson Nascimento, and Andreas Winter. Rates for bit commitment and coin tossing from noisy correlation. In *Proceedings of 2004 IEEE International Symposium on Information Theory*, pages 47–47, June 2004.
- JS00. Richard Jozsa and Jürgen Schlienz. Distinguishability of states and von neumann entropy. *Phys. Rev. A*, 62(1):012301, Jun 2000.
- Ken04. Adrian Kent. Promising the impossible: Classical certification in a quantum world, 2004. <http://arxiv.org/abs/quant-ph/0409029>.
- Kit03. A. Kitaev. Quantum coin-flipping. presented at QIP’03. A review of this technique can be found in <http://lightlike.com/~carlosm/publ>, 2003.
- Kla04. Hartmut Klauck. On quantum and approximate privacy. *Theory of Computing Systems*, 37(1):221–246, 2004. <http://arxiv.org/abs/quant-ph/0110038>, also in the proceedings of STACS 2002.
- KMR09. Robin Künzler, Jörn Müller-Quade, and Dominik Raub. Secure computability of functions in the it setting with dishonest majority and applications to long-term security. In *Theory of Cryptography Conference (TCC)*, volume 5444 of *Lecture Notes in Computer Science*, pages 238–255. Springer, 2009.
- KNTsZ01. Hartmut Klauck, Ashwin Nayak, Amnon Ta-shma, and David Zuckerman. Interaction in quantum communication and the complexity of set disjointness. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 124–133, 2001.

- Kus92. Eyal Kushilevitz. Privacy and communication complexity. *SIAM J. Discrete Math.*, 5(2):273–284, 1992.
- LC97. Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, April 1997.
- Lo97. Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.
- May97. Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997.
- Moc04. Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *45th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 2–11, 2004.
- Moc05. Carlos Mochon. A large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72:022341, 2005.
- Moc07. Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias, 2007. <http://arxiv.org/abs/0711.4114>.
- NC00. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2000.
- PR94. Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.
- Rab81. M. Rabin. How to exchange secrets by oblivious transfer. Technical report, Harvard Aiken Computation Lab, 1981.
- Rus02. Mary Beth Ruskai. Inequalities for quantum entropy: A review with conditions for equality. *Journal of Mathematical Physics*, 43(9):4358–4375, 2002.
- RW05. Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *Advances in Cryptology—ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 199–216. Springer, 2005.
- RWW06. Renato Renner, Stefan Wolf, and Juerg Wullschlegler. The single-serving channel capacity. In *Proceedings of the International Symposium on Information Theory (ISIT)*. IEEE, July 2006. <http://arxiv.org/abs/cs.IT/0608018>.
- Sot08. Miroslava Sotáková. *The Power Of Two-Party Quantum Cryptography*. PhD thesis, Department of Computer Science, University of Aarhus, Denmark, 2008.
- SR01. R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A*, 65(1):012310, 2001.
- SSS09. Louis Salvail, Miroslava Sotáková, and Christian Schaffner. On the power of two-party quantum cryptography. In *Advances in Cryptology—ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 70–87. Springer, 2009.
- Wie83. Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Original manuscript written circa 1970.
- WR07. Andreas Winter and Renato Renner. Single-shot state merging, 2007. unpublished note.
- WW04. Stefan Wolf and Jürg Wullschlegler. Zero-error information and applications in cryptography. In *IEEE Information Theory Workshop (ITW)*, San Antonio, Texas, October 2004.
- WW05a. Stefan Wolf and Jürg Wullschlegler. New monotones and lower bounds in unconditional two-party computation. In *Advances in Cryptology—CRYPTO ’05*, volume 3621 of *Lecture Notes in Computer Science*, pages 467–477. Springer, 2005.
- WW05b. Stefan Wolf and Jürg Wullschlegler. Oblivious transfer and quantum non-locality. In *International Symposium on Information Theory (ISIT 2005)*, pages 1745–1748, 2005.

A Leakage of Universal Primitives

A.1 Exact calculations

First, we look at the leakage of the embeddings of Rabin String OT (ROT^r).

Theorem A.1. Any embedding of $P_{X,Y}^{\text{rot}^r}$ is at least $(1 - O(r2^{-r}))$ -leaking. For $r = 1$ any embedding is at least $(h(\frac{1}{4}) - \frac{1}{2}) \approx 0.311$ -leaking. Furthermore, the leakage is the same for all embeddings of $P_{X,Y}^{\text{rot}^r}$.

Proof. Let

$$|\psi\rangle = \frac{1}{2^{\frac{r+1}{2}}} \sum_{x \in \{0,1\}^r} e^{i\theta(x,x)} |xx\rangle + \frac{1}{2^{\frac{r+1}{2}}} \left(\sum_{x \in \{0,1\}^r} e^{i\theta(x,\perp)} |x\rangle \right) |\perp\rangle,$$

where \perp denotes an erasure, be a general form of an embedding of $P_{X,Y}^{\text{rot}^r}$.

Define $|\varphi\rangle := \frac{1}{2^{r/2}} \sum_{x \in \{0,1\}^r} e^{i\theta(x,\perp)} |x\rangle$. If Bob receives the value of Alice's string successfully, Alice gets an ensemble $\rho^0 = \frac{1}{2^r} \sum_{x \in \{0,1\}^r} |x\rangle\langle x|$. If an erasure occurs on Bob's side, Alice gets $\rho^1 = |\varphi\rangle\langle\varphi|$. We find $S(A)$ by computing the eigenvalues of $\rho_A := \frac{1}{2}(\rho^0 + \rho^1)$.

Since $\rho^0 = \frac{1}{2^r} \mathbb{I}_A$, $|v\rangle$ is an eigenvector of ρ_A if and only if it is an eigenvector of ρ^1 . If $|v\rangle$ is an eigenvector of ρ^1 then either a) $|v\rangle = e^{i\theta} |\varphi\rangle$ or b) $\langle v|\varphi\rangle = 0$. If a) is the case, then

$$\rho_A |v\rangle = \frac{1}{2}(\rho^0 |v\rangle + \rho^1 |v\rangle) = \frac{1}{2} \left(1 + \frac{1}{2^r} \right) |v\rangle,$$

whereas in the case b),

$$\rho_A |v\rangle = \frac{1}{2}(\rho^0 |v\rangle + \rho^1 |v\rangle) = \frac{1}{2^{r+1}}.$$

The state ρ_A has eigenvalues $\{\frac{1}{2} + \frac{1}{2^{r+1}}, \frac{1}{2^{r+1}}\}$, where $\frac{1}{2^{r+1}}$ has multiplicity $2^r - 1$. $S(A)$ can then be computed as follows:

$$\begin{aligned} S(A) &= - \left(\frac{1}{2} + \frac{1}{2^{r+1}} \right) \log \left(\frac{1}{2} + \frac{1}{2^{r+1}} \right) + \frac{2^r - 1}{2^{r+1}} (r + 1) \\ &= \left(\frac{1}{2} + \frac{1}{2^{r+1}} \right) \left(1 - \frac{1}{\ln 2 \cdot 2^r} + o\left(\frac{1}{2^r}\right) \right) + \frac{r+1}{2} - \frac{r+1}{2^{r+1}} = \frac{r}{2} + 1 - O\left(\frac{r}{2^r}\right). \end{aligned}$$

Since $I(X;Y) = \frac{r}{2}$, for the leakage we get:

$$\Delta_\psi(P_{X,Y}^{\text{rot}^r}) = S(A) - I(X;Y) = 1 - O\left(\frac{r}{2^r}\right).$$

As we can see, the leakage does not depend on the phase-function θ . □

In the following theorem we minimize the leakage of an embedding of $P_{X,Y}^{\text{ot}}$.

Theorem A.2. Any $|\psi\rangle \in \mathcal{E}(P_{X,Y}^{\text{ot}})$ is at least $\frac{1}{2}$ -leaking. The leakage is minimized by the canonical embedding.

Proof. Let

$$|\psi\rangle = \frac{1}{2\sqrt{2}} \sum_{x_0, x_1, c \in \{0,1\}} e^{i\theta(x_0 x_1, c x_c)} |x_0 x_1\rangle |c x_c\rangle$$

be a regular embedding of $P_{X,Y}^{\text{ot}}$. Without loss of generality assume that $\theta(00,00) = 0$. Notice that for the local phase-changing transformations

$$\begin{aligned} U^A &:= |00\rangle\langle 00| + \exp(i\theta(01,00))|01\rangle\langle 01| + \exp(i(\theta(10,10) - \theta(00,10)))|10\rangle\langle 10| \\ &\quad + \exp(i(\theta(10,10) + \theta(11,01) - \theta(00,10) - \theta(10,01)))|11\rangle\langle 11|, \\ U^B &:= |00\rangle\langle 00| + \exp(i(\theta(00,10) + \theta(10,01) - \theta(10,10)))|01\rangle\langle 01| \\ &\quad + \exp(i\theta(00,10))|10\rangle\langle 10| + \exp(i(\theta(01,11) - \theta(01,00)))|11\rangle\langle 11|, \end{aligned}$$

we get

$$U^A \otimes U^B |\psi\rangle = |\psi'\rangle = \frac{1}{2}(|0+\rangle|00\rangle + |1+\rangle|01\rangle + |+0\rangle|10\rangle + \frac{|0\rangle + e^{i\omega}|1\rangle}{\sqrt{2}}|1\rangle|11\rangle),$$

where $\omega = \theta(00, 10) + \theta(01, 00) + \theta(10, 01) + \theta(11, 11) - \theta(01, 01) - \theta(10, 10) - \theta(11, 01)$.

Let A' denote Alice's quantum system for Alice and Bob sharing $|\psi'\rangle$. Since $S(A) = S(A')$, we can minimize $S(A')$ in order to minimize $S(A)$. Assume that Alice and Bob share $|\psi'\rangle$. For Bob's selection bit $c = 0$, Alice gets an ensemble $\rho_0 = \frac{1}{2}(|0+\rangle\langle 0+| + |1+\rangle\langle 1+|)$, whereas for $c = 1$, she gets $\rho_1 = \frac{1}{2}(|+0\rangle\langle +0| + (|01\rangle + e^{i\omega}|11\rangle)(\langle 01| + e^{-i\omega}\langle 11|))$, where $\rho_{A'} = \frac{1}{2}(\rho_0 + \rho_1)$. By solving the characteristic equation of $\rho_{A'}$ we get the set of eigenvalues $\{\frac{1}{4}(1 \pm \cos \frac{\omega}{4}), \frac{1}{4}(1 \pm \sin \frac{\omega}{4})\}$. $S(A')$ can then be expressed as follows:

$$S(A') = 1 + \frac{h(\frac{1-\cos(\omega/4)}{2}) + h(\frac{1-\sin(\omega/4)}{2})}{2}.$$

By computing the second derivative of $f(x) = h(\frac{1-\sqrt{x}}{2})$, we get that $f''(x) \leq 0$ in $[0, 1]$, implying that f is concave in $[0, 1]$. For $\alpha \in [0, 1]$, Jensen's inequality yields $\frac{f(0)+f(1)}{2} \leq f(\alpha)$, and therefore, $\frac{f(0)+f(1)}{2} \leq \frac{f(\alpha)+f(1-\alpha)}{2}$. Consequently, the minimum of $h(\frac{1-\cos(\omega/4)}{2}) + h(\frac{1-\sin(\omega/4)}{2}) = f(\cos^2 \frac{\omega}{4}) + f(\sin^2 \frac{\omega}{4})$ is achieved for $\omega = 0$ and in this case, $S(A') = \frac{3}{2}$.

Finally, we can conclude that the leakage is minimal for the canonical embedding and $\Delta_\psi(P_{X,Y}) = S(A) - I(X; Y) = S(A') - I(X; Y) \geq \frac{3}{2} - 1 = \frac{1}{2}$. \square

There is also a more direct way to interpret this quantity in the case of the canonical embedding $|\psi_0\rangle$ for $P_{X,Y}^{\text{or}}$: If Alice and Bob share a single copy of $|\psi_0\rangle$ then there exist POVMs for both of them which reveal Bob's selection bit to Alice, and the XOR of Alice's bits to Bob, both with probability $\frac{1}{2}$. Let $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ denote the Bell states, and $|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Observe that the canonical embedding $|\psi_0\rangle$ of $P_{X,Y}^{\text{or}}$ can be expressed as follows:

$$|\psi_0\rangle = \frac{1}{2}|\Psi^-\rangle \otimes \frac{|\Psi^-\rangle - |\Phi^-\rangle}{\sqrt{2}} + \frac{1}{2}|\Phi^-\rangle \otimes \frac{|\Psi^+\rangle - |\Phi^+\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}|++\rangle|++\rangle.$$

In order to get the value $x_0 \oplus x_1$ of Alice's bits x_0 and x_1 , Bob can use POVM $\mathbf{B} = \{\mathbf{B}_0, \mathbf{B}_1, \mathbf{B}_?\}$ where $\mathbf{B}_0 := \frac{1}{2}(|\Psi^-\rangle - |\Phi^-\rangle)(\langle \Psi^-| - \langle \Phi^-|)$, $\mathbf{B}_1 := \frac{1}{2}(|\Psi^+\rangle - |\Phi^+\rangle)(\langle \Psi^+| - \langle \Phi^+|)$, and $\mathbf{B}_? := |++\rangle\langle ++|$. It is easy to verify that Bob gets outcome \mathbf{B}_z for $z \in \{0, 1\}$ (in which case $x_0 \oplus x_1 = z$ with certainty) with probability $\frac{1}{2}$. Alice's POVM can be defined as $\mathbf{A} = \{\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_?\}$ where $\mathbf{A}_0 := |--\rangle\langle --|$, $\mathbf{A}_1 := |+-\rangle\langle +-|$, and $\mathbf{A}_? := \mathbb{I}_2 - \mathbf{A}_0 - \mathbf{A}_1$. By inspection we easily find that the probability for Alice to get Bob's selection bit is $1 - \text{tr}((\mathbf{A}_? \otimes \mathbb{I}_2)|\psi_0\rangle\langle \psi_0|) = \frac{1}{2}$. For any regular embedding of $P_{X,Y}^{\text{or}}$ we can construct similar POVMs revealing the XOR of Alice's bits to Bob and Bob's selection bit to Alice with probability strictly more than $\frac{1}{4}$.

A.2 Lower Bounds

Theorem A.3. *Any embedding $|\psi\rangle$ of $P_{X,Y}^{\text{or}^r}$ is $(1 - O(r2^{-r}))$ -leaking.*

Proof. We use Theorem 4.13 to show that any (regular) embedding of $P_{X,Y}^{\text{ort}^r}$ leaks at least as much as some regular embedding of $P_{X,Y}^{\text{rot}^r}$. Let (A_0, A_1) and B denote Alice's and Bob's respective registers. Then $|\psi\rangle_{A_0 A_1 B} \in \mathcal{E}(P_{X,Y}^{\text{ort}^r})$ can be written in the form:

$$|\psi\rangle = \frac{1}{2^{r/2}} \sum_{x \in \{0,1\}^r} |x\rangle^{A_1} |\psi^x\rangle_{A_0 B},$$

where each

$$|\psi^x\rangle = \frac{1}{2^{(r+1)/2}} \sum_{x' \in \{0,1\}^r} \left(e^{i\theta(x',x,0)} |x'\rangle^{A_0} |0, x'\rangle^B + e^{i\theta(x',x,1)} |x'\rangle^{A_0} |1, x'\rangle^B \right)$$

can be viewed as a regular embedding of $P_{X,Y}^{\text{rot}^r}$. According to Theorem 4.13 and Theorem A.1, we get that

$$\Delta_{P_{X,Y}^{\text{ort}^r}} \geq \Delta_{P_{X,Y}^{\text{rot}^r}} = 1 - O(r/2^r).$$

□

Theorem A.4. *If $p < \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 0.1464$ then $\Delta_{P_{X,Y}^{\text{ort}^p}} \geq \frac{(1/2 - p - \sqrt{p(1-p)})^2}{8 \ln 2}$.*

Proof. Before starting with the actual proof, we formulate a useful statement, relating two measures of uncertainty of a quantum ensemble.

Theorem A.5 (Average Encoding Theorem [KNTsZ01]). *Let E denote a quantum system storing the quantum part of a cq-state $\rho_{XE} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \rho_E^x$. Then*

$$\sum_x P_X(x) \|\rho_E - \rho_E^x\|_1 \leq \sqrt{2(\ln 2) S(X; E)}.$$

In order to prove Theorem A.4, we first notice that for any regular embedding of $P_{X,Y_0 Y_1}$ such that Y_0 and Y_1 are independent, it holds that

$$S(A; Y_0 Y_1) \geq S(A; Y_0) + S(A; Y_1). \quad (19)$$

We can write

$$\begin{aligned} S(A; Y_0) + S(A; Y_1) &= H(Y_0) + H(Y_1) - S(Y_0|A) - S(Y_1|A) \\ &= H(Y_0 Y_1) - S(Y_0|A) - S(Y_1|A) \\ &\leq H(Y_0 Y_1) - S(Y_0 Y_1|A) = S(A; Y_0 Y_1), \end{aligned}$$

which proves Inequality (19).

Let X, Y_0, Y_1 be random variables corresponding to Alice's pair of bits, Bob's selection bit, and its value, respectively. For $P_{X,Y}^{\text{ort}^p}$ we have that $I(X; Y_0 Y_1) = 1 - h(p)$. As the selection bit Y_0 and the value Y_1 are independent, we can use (19) to lower bound $S(A; Y_0 Y_1)$ as follows

$$S(A; Y_0 Y_1) \geq S(A; Y_0) + S(A; Y_1) \geq S(A; Y_0) + (1 - h(p)).$$

Hence, for computing the lower bound on $S(A; Y_0 Y_1)$, we only need to compute the lower bound on $S(A; Y_0)$. A state $|\psi\rangle \in \mathcal{E}(P_{X,Y}^{\text{ort}^p})$ can be written as

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|\psi_0\rangle^{AB_1} |0\rangle^{B_0} + |\psi_1\rangle^{AB_1} |1\rangle^{B_0}).$$

Let $\rho_A^0 := \text{tr}_{B_1} |\psi_0\rangle\langle\psi_0|$ and $\rho_A^1 := \text{tr}_{B_1} |\psi_1\rangle\langle\psi_1|$. By applying Theorem A.5 from above, we get that

$$\|\rho_A^0 - \rho_A^1\|_1 \leq \sqrt{8(\ln 2)S(A; Y_0)},$$

and therefore,

$$\frac{\|\rho_A^0 - \rho_A^1\|_1^2}{8 \ln 2} \leq S(A; Y_0). \quad (20)$$

The trace norm of $\rho_A^0 - \rho_A^1$ yields an upper bound on the entries of the matrix:

$$|(\rho_A^0 - \rho_A^1)_{ij}| \leq \|\rho_A^0 - \rho_A^1\|_1. \quad (21)$$

We can write the state $|\psi\rangle$ in the form:

$$|\psi\rangle = \frac{1}{2} \sum_{y_0, y_1} |\varphi^{y_0, y_1}\rangle_A |y_0, y_1\rangle_{B_0 B_1},$$

where

$$\begin{aligned} |\varphi_{0,y}\rangle &= \sqrt{\frac{1-p}{2}} \sum_{x=0}^1 e^{i\theta(y, x, 0, y)} |y, x\rangle_A |0, y\rangle_{B_0 B_1} + \sqrt{\frac{p}{2}} \sum_{x=0}^1 e^{i\theta(y, x, 0, 1-y)} |y, x\rangle_A |0, 1-y\rangle_{B_0 B_1} \\ |\varphi_{1,y}\rangle &= \sqrt{\frac{1-p}{2}} \sum_{x=0}^1 e^{i\theta(x, y, 1, y)} |x, y\rangle_A |1, y\rangle_{B_0 B_1} + \sqrt{\frac{p}{2}} \sum_{x=0}^1 e^{i\theta(x, y, 1, 1-y)} |x, y\rangle_A |1, 1-y\rangle_{B_0 B_1}. \end{aligned}$$

By evaluating the individual matrix entries of $(\rho_A^0 - \rho_A^1)$ we get a simple lower bound on $|(\rho_A^0 - \rho_A^1)_{ij}|$ for $i \neq j \in \{0, \dots, 3\}$:

$$|(\rho_A^0 - \rho_A^1)_{ij}| \geq \frac{1-2p}{4} - \frac{\sqrt{(1-p)p}}{2} \quad (22)$$

hence, from (21) follows that

$$\|\rho_A^0 - \rho_A^1\|_1 \geq \frac{1-2p}{4} - \frac{\sqrt{(1-p)p}}{2},$$

yielding due to (19) and (20) that

$$S(A; Y_0 Y_1) \geq 1 - h(p) + S(A; Y_0) \geq 1 - h(p) + \frac{(1/2 - p - \sqrt{(1-p)p})^2}{32 \ln 2}.$$

The lower-bound is non-trivial if $1/2 - p - \sqrt{(1-p)p} > 0$, which is true for $p < \frac{1}{2} - \frac{1}{2\sqrt{2}}$. The results yields the following lower-bound on the leakage of $P_{X,Y}^{\text{otp}}$:

$$\Delta_{P_{X,Y}^{\text{otp}}} \geq \frac{(1/2 - p - \sqrt{(1-p)p})^2}{32 \ln 2}.$$

However, this lower-bound is very loose, since for $p = 0$ we get that

$$\Delta_{P_{X,Y}^{\text{otp}}} \geq \frac{1}{128 \ln 2} \approx 0.011,$$

which is much weaker than the optimal

$$\Delta_{P_{X,Y}^{\text{otp}}} \geq \frac{1}{2}.$$

□

It remains to mention that by using more careful analysis of the phases of $|\varphi_{0,y}\rangle$ and $|\varphi_{1,y}\rangle$, the lower bound on the absolute value of the outside-diagonal entries from (22) can be improved, yielding a non-trivial lower bound on the leakage for $p > 0.1464$ and eventually, even for any $p < 1/4$.